إريك شميدت
ERIC SCHMIDT
الرئيس التنفيذي لشركة غوغل

جاريد كوين
JARED COHEN
مدير قسم «الأفكار» في شركة غوغل

الأكثر مبيعاً على قائمة «نيويورك تايمز» وفي العالم

العصر الرقمي الجديد

THE NEW DIGITAL AGE

إعادة تشكيل مستقبل الأفراد والأمم والأعمال


الدار العربية للعلوم ناشرون
Arab Scientific Publishers, Inc.

العصر الرقمي الجديد

إعـادة تشكيل
مستقبل الأفـراد والأمم والأعمـال

تأليف
إريك شميدت و جاريد كوين

ترجمة
أحمد حيدر

مراجعة وتحرير
مركز التعريب والبرمجة





يتضمن هذا الكتاب ترجمة الأصل الإنكليزي
The New Digital Age

حقوق الترجمة العربية مرخّص بها قانونياً من الناشر
Alfred A. Knopf, New York

بمقتضى الاتفاق الخطي الموقّع بينه وبين الدار العربية للعلوم ناشرون، ش.م.ل.

الطبعة الأولى

1434 هـ - 2013 م

ISBN: 978-614-02-0758-5



عين التينة، شارع المفتي توفيق خالد، بناية الريم
هاتف: (1-961+) 785107 - 785108 - 786233
ص.ب: 13-5574 شوران - بيروت 2050-1102 - لبنان
فاكس: (1-961+) 786230 - البريد الإلكتروني: bachar@asp.com.lb
الموقع على شبكة الإنترنت: http://www.asp.com.lb

التنضيد وفرز الألوان: أبجد غرافيكس، بيروت - هاتف (9611+) 785107
الطباعة: مطابع الدار العربية للعلوم، بيروت - هاتف (9611+) 786233

مقدمة

الإنترنت من الأشياء القليلة التي بناها البشر من دون أن يفهموها حق الفهم. فما بدأ كوسيلة لنقل المعلومات إلكترونياً (من حاسب بحجم غرفة إلى حاسب آخر بحجم مشابه)، تحول إلى منفذ متعدد الوجوه للطاقة البشرية والتعبير البشري منتشر في كل مكان. فهي شيء غير ملموس، ولكنها في الوقت نفسه في حالة تغير دائم تزداد معها نمواً وتعقيداً بمرور كل ثانية. إنها مصدر خير وفير، ولكنها قد تكون أيضاً مصدراً لشرور مروعة. إن كل ما شهدناه حتى الآن ليس سوى بداية لأثرها على المسرح العالمي.

لم يشهد التاريخ تجربة تضاهي الإنترنت في فوضويتها. فمئات الملايين من البشر يعملون كل دقيقة على إنتاج قدر غير مسبوق من المحتوى الرقمي في عالم شبكي، كما يعملون على استهلاكه. وهذه القدرة الجديدة على التعبير بحرية، وعلى نقل المعلومات بحريّة أيضاً هي التي أنتجت المشهد الافتراضي الغني الذي نعرفه اليوم. فكّر بجميع مواقع الوب التي قمت بزيارتها، وجميع رسائل البريد الإلكتروني التي أرسلتها، وجميع القصص التي قرأتها على الشبكة، وبجميع الحقائق التي تعلمتها، والقصص الخيالية التي مررت بها أو كشفت زيفها. فكّر في كل ما نشأ وتحقق عبر هذه المنصة؛ بكل علاقة تشكلت، وكل رحلة تم التخطيط لها، وكل فرصة عمل تم العثور عليها، وكل حلم وُلِد. فكّر أيضاً في ما قد يحدث عند غياب التحكم: من الاحتيال عبر الإنترنت، وحملات التنمّر، ومواقع مجموعات الكراهية، وغرف محادثة الإرهابيين. هذه هي الإنترنت؛ إنها أكبر فضاء خارج عن السيطرة في العالم.

مع نمو هذا الفضاء سيتغير فهمنا لكل جانب من جوانب الحياة تقريباً؛ بدءاً من تفاصيل حياتنا اليومية، ومروراً بالأسئلة الأكثر عمقاً المتعلقة بالهوية والعلاقات، بل ووصولاً إلى الأمن أيضاً. فالعوائق الأزلية التي لطالما وقفت في وجه التواصل البشري، كالجغرافيا واللغة ومحدودية المعلومات، لا تنفك تتهافت جميعها بفضل التقانة، لتبرز بذلك موجة جديدة من الإبداع ومن الإمكانيات البشرية. ويدفع التبني الجماهيري للإنترنت نحو أكثر التحولات الاجتماعية والثقافية والسياسية إثارة عبر التاريخ، وستكون آثار التغيير هذه المرة - على خلاف الحقبات السابقة - شاملة كلياً. إذ لم يحدث في التاريخ مطلقاً أن توفر بين أيدي كل هذا القدر من الناس - من أماكن متنوعة جداً - كل هذا القدر من القوة. وإذا لم تكن هذه هي أول ثورة تقانية في تاريخنا، فإنها الأولى التي ستمكن أي شخص تقريباً من امتلاك المحتوى بالزمن الحقيقي، وتطويره ونشره من دون أن يكون عليه اللجوء إلى وسطاء.

كل ذلك يحصل ونحن بالكاد قد تجاوزنا الحواجز الأولى؛ حيث كان تقدم تقانات الاتصال وتكاثرها يجريان بسرعة غير مسبوقة. فخلال العقد الأول من القرن الحادي والعشرين ارتفع عدد المتصلين في العالم من 350 مليوناً إلى أكثر من مليارين، وفي الفترة نفسها ارتفع عدد مشتركي الهاتف الخلوي من 750 مليوناً إلى

أكثر من 5 مليارات (وهو الآن أكثر من 6 مليارات). لقد وصلت هذه التقانات في انتشارها إلى أقاصي المعمورة؛ محققة معدل انتشار متسارعاً في بعض الأماكن.

وبحلول عام 2025 سيكون معظم سكان الأرض قد انتقلوا خلال جيلٍ واحد من مرحلةٍ لم تكن تتاح لهم فيها أية معلوماتٍ غير مفلترة إلى مرحلةٍ صار بإمكانهم فيها الوصول إلى جميع المعلومات في العالم عبر جهازٍ بحجم الكف. وإذا تم الحفاظ على المسيرة الحالية للابتكار التقاني فسيكون معظم البشر - من المليارات الثمانية المتوقع وجودهم على سطح الأرض حينئذ - متصلين بالإنترنت.

ستتاح إمكانية الاتصال أكثر فأكثر على جميع مستويات المجتمع، وسيتمكن الناس من الاتصال بشبكات إنترنت لاسلكية منتشرة في كل مكان، وسنكون أكثر فعالية وأكثر إنتاجية وأكثر إبداعاً. وفي العالم النامي، ستعمل كلٌ من نقاط الاتصال اللاسلكية العمومية والشبكات المنـزلية عالية السرعة على تقوية الأخرى؛ لتتوسع بذلك تجربة الاتصال بالإنترنت إلى أماكن لا تتوفر للناس فيها اليوم وسائل اتصال - حتى عبر الهواتف الأرضية - وستقفز المجتمعات جيلاً كاملاً من التقانة إلى الأمام.

في نهاية المطاف، سيتم بيع تجهيزات التقانة التي نراها اليوم عجيبة في أسواق الخردوات، تماماً كما كان مصير الهواتف القديمة ذات الأقراص الدوارة.

ومع اتساع انتشار هذه الأدوات ستزداد أيضاً سرعاتها وقدراتها الحسابية. فوفقاً لقانون مور - وهو قانون تجريبـي في الصناعة التقانية - تتضاعف سرعة رقائق المعالجات (لوحات الدارات الصغيرة، تلك التي تشكل العمود الفقري لكل جهازٍ حاسب) كل ثمانية عشر شهراً، أي إن الحاسب عام 2025 سيكون أسرع بنحو 64 مرة مما هو عليه عام 2013. وثمة قانون توقعي آخر من عالم الضوئيات (يتعلق بنقل المعلومات) يخبرنا أن كمية البيانات الواردة من كابلات الألياف الضوئية - وهي أسرع أشكال الاتصال - تتضاعف كل تسعة أشهر. وحتى لو كانت لهذه القوانين حدودٌ طبيعية، فإن بشرى النمو الأسّي تكشف عن إمكانياتٍ في مجالات الرسوميات والواقع الافتراضي ستجعل تجربة الاتصال بالإنترنت حقيقيةً إلى أقصى الحدود. الأمر أشبه بأن تكون لديك تقانة المركب التجسيمي (هولو دك) من عالم ستار تراك - وهي بيئة واقعٍ افتراضي يستخدمها من هم على متن سفينة - لكنها قادرةٌ في الوقت نفسه على عرض مشهدٍ، أو على إعادة إنتاج أداءٍ شهيرٍ لإلفيس بريسلي أمام عينيك. المحطات القادمة في مسيرة تطورنا التقاني تعِدُ بتحويل عددٍ كبيرٍ من مفاهيم الخيال العلمي الشائعة إلى حقائق علمية؛ كالسيارات من دون سائق، أو الحركة الروبوتية التي يُتحكم بها بالأفكار، أو الذكاء الصنعي، أو إدماج الواقع الرقمي من خلال إنتاج كساء بصري يظهر بيئة رقمية. مثل هذه التطورات سترافق مفردات عالمنا الطبيعي وتحسنها.

هذا مستقبلنا، وقد بدأت ملامح هذه الأشياء الرائعة تظهر فعلاً؛ مما يجعل العمل في صناعة التقانة اليوم مثيراً جداً؛ ليس فقط بفضل الفرصة السانحة لنا لاختراع أجهزةٍ جديدةٍ مذهلة وبنائها، ولا نتيجة التحديات التقانية والفكرية التي سنحاول التغلب عليها، بل لما ستعنيه هذه التطورات بالنسبة إلى العالم.

تقدم تقانات الاتصال فرصاً لإنجاز تقدم ثقافي إلى جانب التقدم التقني. فطريقة

تفاعلنا مع بعضنا ونظرتنا إلى بعضنا ستتأثر دائماً بالعالم الشبكي المحيط بنا وستسير على خطاه. كما ستسمح لنا نـزعة الذاكرة الانتقائية بتبني عاداتٍ جديدة بسرعة، ونسيان الطرق التي كنا نمارس بها عاداتنا في السابق. فمن الصعب اليوم تخيل الحياة من دون أجهزةٍ نقالة. وفي زمنٍ تتواجد فيه الهواتف الذكية في كل مكان، أصبح لديك تأمينٌ ضد النسيان؛ فبإمكانك الوصول إلى عالمٍ كاملٍ من الأفكار (رغم أن بعض الحكومات تجعل ذلك أمراً صعباً). ودائماً ثمة شيء ما يحتل انتباهك، ولو كان من الصعب أحياناً أن تجد فائدة في القيام بذلك. والهاتف الذكي لم يطلق عليه هذا الاسم عبثاً.

مع استمرار الاتصالات العالمية في تقدمها غير المسبوق، سيتوجب على الكثير من المؤسسات والبنى الهرمية التأقلم معها، وإلا فإنها ستجازف بأن تصبح قديمة ومنفصلةً عن المجتمع الحديث. وليست تلك النـزاعات التي نشهدها اليوم في الكثير من مجالات الأعمال - الكبيرة منها والصغيرة - سوى أمثلةٍ على التحول الجذري القادم على المجتمع؛ إذ ستستمر تقانات الاتصال بتغيير مؤسساتنا من الداخل ومن الخارج، وستزداد إمكانية وصولنا إلى أناسٍ خارج حدودنا ومجموعاتنا اللغوية، وسيزداد ارتباطنا بهم حيث نشاركهم الأفكار ونصرف معهم الأعمال ونبني معهم علاقاتٍ أصيلة.

سيجد معظمنا أنفسهم - على نحو مضطردٍ - يعيشون في عالمين في آنٍ معاً. فكل منا سيعيش في العالم الافتراضي نوعاً ما من التواصل، وسيكون ذلك سريعاً وعبر تشكيلةٍ كبيرة من الوسائل والأجهزة. أما في العالم المادي، فسنظل نصارع الجغرافيا، وعشوائية الولادة (حيث يولد البعض أغنياء في بلدانٍ غنية، بينما يبقى معظم الأشخاص فقراء في بلدانٍ فقيرة)، وسوء الحظ، والجانبين الخيّر والشرير من الطبيعة الإنسانية. سنسعى في هذا الكتاب إلى استعراض الطرق التي يستطيع العالم الافتراضي فيها أن يجعل العالم الفيزيائي أفضل أو أسوأ، أو ربما مختلفاً فقط. وربما يقوم هذان العالمان أحياناً بتقييد أحدها الآخر، وقد يتصادمان أحياناً أخرى، أو يكثف أحدهما ظواهر العالم الآخر ويسرعها ويفاقمها؛ حيث يتحول الفرق في الدرجة إلى فرقٍ في النوع.

وسيكون أهم أثرٍ لانتشار تقانات الاتصالات على المسرح العالمي متمثلاً في كيفية مساعدتها على إزاحة مركز السلطة بعيداً عن الدول والمؤسسات، حيث ستنقله إلى الأفراد. فغالباً ما كان انتشار تقانات معلومات جديدة عبر التاريخ يقوي موجات متتابعة من البشر على حساب وسطاء السلطة التقليديين، سواء أكانوا الملك أم الكنيسة أم النخب. فالوصول إلى المعلومات وإلى قنوات الاتصال الجديدة كان ولا يزال رديفاً لتوفر فرص المشاركة واستلام زمام المبادرة وإمكانية توجيه الفرد لمسار حياته بقدر أعظم من الاستقلالية.

لعل انتشار الاتصالات - وخصوصاً عبر الهواتف النقالة المزودة باتصال إنترنت - أعمق مثال على هذا التحول في السلطة، لكنه بالتأكيد أكثر الأمثلة شيوعاً؛ على الأقل نتيجة المدى الذي يصل إليه. سيكون التمكين الرقمي بالنسبة للبعض أول تجربة تمكينٍ يمرون بها في حياتهم، وبفضله سيكون صوتهم مسموعاً وسيحسب

حسابهم وسيؤخذون على محمل الجد؛ كل ذلك بفضل جهازٍ رخيصٍ يمكنهم حمله في جيوبهم. ونتيجة لذلك ستجد الحكومات الاستبدادية صعوبة في السيطرة على شعوبها المتصلة حديثاً، كما ستجد صعوبة في قمعها والتأثير عليها، بينما ستجبر الحكومات الديموقراطية على أخذ رأي المزيد من الأصوات (أفراد ومنظمات وشركات) بعين الاعتبار عند قيامها بأعمالها. وما من شك في أن الحكومات ستجد دائماً طرقاً تستغل فيها المستويات الجديدة من الاتصالات لصالحها، لكن بنية تقانة الشبكات الحالية اليوم منحازةٌ لصالح المواطنين بالفعل، وبطرقٍ سنستكشفها في ما يلي.

فهل سيؤدي انتقال السلطة إلى الأفراد بهذه الطريقة في النهاية إلى عالم أكثر أماناً أم إلى عالم أكثر خطورة؟ لا يسعنا سوى أن ننتظر ونرى؛ فما شهدناه حتى الآن من وقائع يولِّدها التواصل في العالم ليس سوى البداية، وسيكون بعض هذه الوقائع حسناً وسيئاً ومقلقاً. كلانا نحن المؤلفان استكشفنا هذه المسألة من وجهتي نظر مختلفتين؛ الأول كعالم معلوماتية ومدير تنفيذي، والآخر كخبير في السياسة الخارجية والأمن القومي. وكلانا نعلم أن الجواب ليس واضحاً ومعروفاً، فالمستقبل سيتشكل وفقاً لطريقة تعامل الدول والشركات والمؤسسات مع مسؤولياتها الجديدة، كذلك هي حال المواطنين.

كان منظرو العلاقات الدولية في الماضي يتجادلون حول طموحات الدول، فكان بعضهم يرى أن الدول تمارس سياسات محلية وخارجية تهدف إلى تعظيم نفوذها وأمنها. بينما اقترح آخرون أن هناك عوامل إضافية، مثل التجارة وتبادل المعلومات، تؤثر أيضاً في سلوك الدولة. وإذا كانت طموحات الدول لن تتغير فإن مفهومها لطريقة تحقيقها هو الذي سيتغير؛ إذ ستترتب عليه ممارسة نسختين من سياساتها المحلية والخارجية، تكون النسخة الأولى مخصصةً للعالم المادي "الحقيقي"، بينما تركز الثانية على العالم الافتراضي الموجود على الإنترنت. وقد تبدو هاتان السياستان متناقضتين في بعض الأحيان، فقد تمارس الحكومة القمع في إحدى المملكتين بينما تسمح بسلوكياتٍ معينة في الأخرى. وقد تلجأ إلى الحرب في الفضاء الرقمي بينما تحافظ على السلام في العالم المادي. لكن هاتين السياستين ستجسدان سعي هذه الدول إلى التعامل مع التهديدات والتحديات الجديدة التي تحيق بسلطتها والتي أصبحت ممكنة من خلال الاتصالات.

أما بالنسبة إلى المواطنين فسيعني التواجد على الإنترنت حيازة هويتين؛ إحداهما في العالم المادي والأخرى في العالم الافتراضي. وستطغى هوية كل منهم الافتراضية على هويته الأخرى بطرق متعددة لأن الآثار التي سيتركونها ستبقى محفورة في الشبكة إلى الأبد. وبما أن ما ننشره وما نرسله بالبريد الإلكتروني وما ندونه وما نشاركه عبر الشبكة يشكل الهوية الافتراضية بالنسبة إلى الآخرين، فإن أشكالاً جديدة من المسؤولية الجماعية ستفرض وجودها بلا شك.

فبالنسبة إلى المنظمات والشركات، ستجلب الاتصالات العالمية معها الفرص والتحديات. إذ سيكون هناك مستوى جديد من المحاسبة يحركه الناس، وسيجبر اللاعبون على إعادة التفكير بعملياتهم الموجودة مسبقاً، وعلى تكييف خططهم مع

المستقبل بأن يغيروا طريقة ممارستهم للأشياء، وطريقة تقديمهم لنشاطاتهم أمام الجمهور أيضاً. كما سيواجهون منافسين جدداً بعد أن يجعل انتشار التقانة ميدان المنافسة مفتوحاً أمام المعلومات، وبالتالي الفرص.

لن يكون أي شخص في المستقبل - من أكثر الناس نفوذاً إلى أضعفهم - معزولاً عما سيكون في كثيرٍ من الحالات تغيرات تاريخية.

كنا قد التقينا للمرة الأولى في خريف عام 2009، في ظروفٍ سهلت تشكل عروة الصداقة بيننا بسرعة، فقد كنا في بغداد نسعى مع العراقيين للإجابة عن السؤال الحاسم حول قدرة التقانة على مساعدتهم على إعادة إعمار مجتمعهم. وخلال تنقلنا في المدينة، ومقابلتنا وزراء الحكومة والقادة العسكريين والدبلوماسيين والمقاولين العراقيين، كانت أمامنا أمةٌ بدت فرص تعافيها ونجاحها في المستقبل وكأنها معلقة بخيط رفيع. وكانت الرحلة التي قام بها إيريك إلى العراق أوّل رحلة يقوم بها مديرٌ عام لشركة تقانة مدرجة على قائمة فورتشن 500 إلى هناك، وكان ثمة أسئلة كثيرة حول سبب وجود غوغل هناك. ففي ذلك الوقت لم نكن نحن أنفسنا نعلم على وجه اليقين ما الذي قد تواجهه غوغل هناك، أو ما الذي بإمكانها تحقيقه.

لكن الجواب سرعان ما صار جلياً، فأينما نظرنا كنا نرى أجهزة نقالة. وقد فاجأنا ذلك، فقد كان العراق في ذلك الوقت منطقة حرب لما يزيد على ست سنوات بعد سقوط صدام حسين الذي كان قد منع استخدام الأجهزة النقالة. وجاءت الحرب لتجهز على البنية التحتية المادية للعراق؛ فلم يكن المصدر المستقر للغذاء أو الماء أو الكهرباء متوفراً لمعظم الناس، وحتى إن البضائع الأساسية كانت مرتفعة الأسعار إلى حدٍّ تعجيزي. وكانت الأنقاض متجمعة في بعض الأماكن ولم ترحّل لسنوات. والأخطر من ذلك أن أمن الناس لم يكن مضموناً، سواء أكانوا من كبار الضباط أم من أصحاب المتاجر العاديين. لذا، كان المرء يتوقع أن تكون الهواتف النقالة آخر بند يمكن أن يظهر على لائحة المهام الطويلة المدرجة لذلك البلد. إلا أننا سرعان ما أدركنا أن العراقيين - بالرغم من المشكلات الملحة في حياتهم - يولون التقانة أولوية خاصة.

لم يكن العراقيون يقتنون التقانة ويثمنونها وحسب، بل كانوا يدركون أيضاً قدرتها الهائلة على تحسين حياتهم وتحقيق مستقبلٍ أفضل لبلادهم المدماة. فقد عبّر المهندسون والمقاولون الذين قابلناهم عن يأسهم الكبير لعدم قدرتهم على مساعدة أنفسهم، وكانوا يعلمون مسبقاً ما الذي ينقصهم: كهرباء مستقرة، وما يكفي من عرض الحزمة للاتصالات السريعة والأدوات الرقمية، وما يكفي من رأس المال التأسيسي للنهوض بأفكارهم من الحضيض.

كانت تلك أول رحلةٍ لإيريك إلى منطقة حرب، أما بالنسبة إلى جيريد فكانت واحدة من أسفاره التي لا تحصى. لكننا خرجنا بانطباعٍ؛ وهو أن شيئاً ما يتغير في العالم بشكل جذري. فإذا كان العراقيون المنهكون من الحرب لا يرون إمكانيات التقانة وحسب بل يعرفون أيضاً ما يريدون أن يفعلوه بها، فكم من ملايين البشر الآخرين لديهم الحافز والمعرفة الأساسية لكن لا تتوافر بين أيديهم الاتصالات

اللازمة؟ وفي تلك الرحلة، وجد جيري تأكيداً على أن الحكومات متخلفة على نحو خطير في ما يتعلق بتوقع التغيرات، وعلى أنها تخشاها أيضاً، وعلى أنها لا ترى الإمكانيات التي تفتحها هذه الأدوات الجديدة للتعامل مع التحديات القادمة. وأكد إيريك شعوره بأن صناعة التقانة كان أمامها من المشاكل الواجب حلها والزبائن الواجب تخديمهم أكثر بكثير مما قد يدرك أي شخص.

خلال الأشهر التي تلت زيارتنا، بات واضحاً لنا أن ثمة هوة تفصل بين أولئك الذين يفهمون التقانة وأولئك المسؤولين عن أكثر المشكلات الجيوسياسية تعقيداً في العالم، ولم يقم أحد ببناء جسر بين الطرفين، إلا أن التعاون بين صناعة التقانة والقطاع العام والمجتمع المدني يطرح إمكانيات هائلة. وخلال تأملنا في انتشار الاتصالات عبر العالم وجدنا نفسينا محاصرين بالأسئلة التي تفرض هذه الهوة طرحها: من سيكون أكثر سلطةً في المستقبل؟ المواطنون أم الدولة؟ هل ستجعل التقانة ارتكاب الأعمال الإرهابية أسهل أم أصعب؟ ما العلاقة بين الخصوصية والأمن؟ وكم سيتوجب علينا أن نضحي حتى نصبح جزءاً من العصر الرقمي الجديد؟ كيف ستتغير الحرب والدبلوماسية والثورة عندما يصبح الجميع متصلين؟ وكيف يمكننا أن نرجح كفة التوازن لصالحنا؟ وعندما تبدأ عملية إعادة بناء المجتمعات المحطمة، ما الذي ستتيح لنا التقانة فعله؟

تعاونا في البداية على كتابة مذكرة لوزيرة الخارجية هيلاري كلينتون حول الدروس التي يمكن استقاؤها من العراق، ثم كانت الصداقة بحد ذاتها تعاوننا الدائم، فقد كانت لدينا نظرةٌ مشتركة إلى العالم في ما يتعلق بالإمكانيات التي تعد بها المنصات التقانية والسلطة الكامنة فيها. وهذه النظرة هي التي تحدد شكل العمل الذي نقوم به بالكامل، سواء أكان داخل غوغل أم خارجها. فنحن نعتقد أن منصات التقانة الحديثة مثل غوغل وفيسبوك وأمازون وأبل أكثر طاقةً بكثير مما يمكن لمعظم الناس أن يدركوه، وأن عالمنا المستقبلي سيكون مرتبطاً على نحوٍ عميق بمدى اعتماد هذه المنصات ونجاحها في المجتمعات في كل مكان؛ فهي تمثل تغيراً حقيقياً في النماذج الفكرية يضاهي ما صاحب اختراع التلفاز، وهي تستمد قوتها من قدرتها على النمو؛ وتحديداً بالسرعة التي تتوسع بها. فباستثناء الفيروسات البيولوجية، ربما لا يكون هناك شيءٌ قادرٌ على الانتشار بهذه السرعة وبهذه الفعالية وبهذه العدوانية كما تفعل هذه المنصات التقنية؛ مما يجعل أولئك الذين يبنونها ويتحكمون بها ويستخدمونها على قدرٍ من السلطة أيضاً. إذ لم يسبق لهذا القدر من البشر أن كانوا متصلين عبر شبكةٍ ذات استجابةٍ لحظية. والإمكانيات التي ينطوي عليها الفعل الجماعي الذي توفره منصات الشبكة التجمعيّة (كمستهلكين أو مبدعين أو مساهمين أو ناشطين بأي شكلٍ من الأشكال) قادرةٌ بالفعل على تغيير قواعد اللعبة. والآثار الشاملة التي بتنا نعتبرها اعتيادية اليوم، مثل مقاطع الفيديو الفيروسية أو منصات التجارة الإلكترونية العالمية، ليست سوى غيضٍ من الفيض القادم.

نظراً للآثار الشاملة التي تفرضها المنصات الرقمية، ستصبح وتيرة التطورات في العصر الرقمي الجديد أعلى بكثير، وسيطال تأثيرها كل جزءٍ من المجتمع، بما

في ذلك السياسات المتبعة والاقتصاد ووسائل الإعلام والأعمال التجارية والمعايير الاجتماعية. وسيقودنا هذا التسارع في التوسع، مصحوباً بالقدرة على التواصل التي تعززها تقانة الإنترنت إلى عصرٍ جديدٍ من العولمة يقوم على عولمة المنتجات والأفكار. ونحن بصفتنا منتمين إلى قطاع التقانة نجد أن من واجبنا استكشاف آثار صناعتنا على حياة الناس وعلى المجتمع - اليوم وفي المستقبل - استكشافاً كاملاً ونـزيهاً. إذ سيترتب على الحكومات على نحوٍ متزايد أن تشرك الأفراد والشركات في وضع القوانين، فهؤلاء يتحركون بخطواتٍ متسارعة، ويوسعون الحدود أحياناً بسرعةٍ أكبر من أن تواكبها القوانين. فالمنصات الرقمية والشبكات والمنتجات التي يتم إصدارها اليوم تتمتع بتأثيرٍ هائل على المستوى العالمي. ولفهم مستقبل السياسة والأعمال والدبلوماسية وغيرها من القطاعات الهامة، يتعين على المرء فهم كيفية دفع التقانة للتغيرات الكبرى في هذه المجالات.

حين بدأنا بتشارك أفكارنا حول المستقبل، شاءت الصدف أن تحدث سلسلة من الأحداث العالمية البارزة التي جاءت كمثالٍ على المفاهيم والمشكلات التي نناقشها بالذات. فقد شنت الحكومة الصينية هجمات سايبرية معقدة على غوغل وعلى العشرات من الشركات الأمريكية الأخرى، وظهر موقع ويكيليكس على المسرح فجأة؛ متيحاً الوصول إلى مئات الآلاف من السجلات الرقمية السرية على مستوى العالم، وأدت هزات أرضية كبيرة في هاييتي واليابان إلى دمار المدن، لكنها أثارت استجابات مبتكرة محركها التقانة. وجاءت ثورات الربيع العربـي لتهز العالم بسرعتها وقوتها وآثار التعبئة المعدية التي رافقتها، فكان كل تطورٍ مضطرب يقدم لنا إمكانيات رؤى جديدة حول المستقبل لنتأملها.

لقد أمضينا قدراً كبيراً من الوقت في مناقشة معنى أحداث كتلك وتبعاتها، محاولين توقع التوجهات التي ستسود والحلول الممكنة من خلال التقانة، وهذا الكتاب هو نتاج تلك المحادثات.

سنعمل في الصفحات القادمة على عرض نظرتنا للمستقبل المليء بالقضايا العالمية المعقدة كالمواطنة والسياسة والحرب والخصوصية، بالإضافة إلى مسائل أخرى، مع التحديات والحلول التي يدفعها صعود القدرة العالمية على التواصل. وحين يكون ذلك ممكناً سنشرح ما يمكن فعله للمساعدة على توجيه هذا الدفق من الأدوات التقانية الجديدة بما يساهم في تحسين عالمنا وإغنائه وتزويده بالمعلومات. لم يكن هناك مناص من التغيير الذي تدفعه التقانة، غير أننا في كل مرحلةٍ سنكون قادرين على فرض قدر من السيطرة على شكله النهائي. وستكون بعض التوقعات التي ستقرأها في الصفحات التالية أشياء كنت تشك فيها منذ وقتٍ طويل لكنك لم تجرؤ على الاعتراف بها (مثل الاستنتاجات المنطقية التي تستتبعها حرب المركبات غير المأهولة التجارية)، بينما سيكون بعضها الآخر جديداً كلياً، ونحن نأمل أن تكون توقعاتنا ونصائحنا حافزاً لك على التفكير.

ليس هذا كتاباً عن الأدوات أو تطبيقات الهاتف الذكي أو الذكاء الاصطناعي - وإن كان كل من هذه المواضيع ستتم مناقشته - فهذا الكتاب عن التقانة، لكنه علاوةً على ذلك كتاب حول البشر، وحول طريقة تفاعلهم مع التقانات في بيئتهم، وطريقة

تطبيقهم لها، وتأقلمهم معها، واستغلالهم لها اليوم وفي المستقبل في جميع أنحاء العالم. يتناول هذا الكتاب قبل كل شيء أهمية الإبقاء على يد بشرية في العصر الرقمي الجديد. فمع جميع الإمكانيات التي تمثلها تقانات الاتصالات يبقى خيار استخدامها للخير أو للشر معتمداً على البشر حصراً. ولندع جانباً كل الأحاديث عن الآلات التي ستسيطر علينا، فما سيحدث في المستقبل منوطٌ بنا وحدنا.

الفصل الأول: كيف سنكون في المستقبل

عما قريب سيصبح كل من على وجه الأرض على اتصال. ومع انضمام خمسة مليارات شخص آخرين إلى العالم الافتراضي، سيعود ازدهار التواصلية الرقمية بمكاسب في مجالات الإنتاج والصحة والتعليم وجودة الحياة وآلاف المجالات الأخرى في العالم المادي. وسينطبق ذلك على كل شخص؛ من نخبة المستخدمين إلى أولئك القابعين في قاعدة الهرم الاقتصادي. لكن كون المرء سيكون له معنى مختلف باختلاف الأشخاص، ويعود سبب ذلك بشكلٍ رئيس إلى المشكلات التي سيتوجب عليهم حلها؛ إذ ستختلف اختلافاً جذرياً من شخصٍ إلى آخر، وما قد يبدو قفزةً صغيرةً إلى الأمام بالنسبة إلى البعض (كشراء هاتفٍ ذكي بسعر لا يتجاوز العشرين دولاراً) قد يحدث أثراً عميقاً بالنسبة إلى مجموعةٍ أخرى يوازي امتلاك سيارة من دون سائق تذهب بها إلى العمل. سيجد الناس أن الاتصالية ستجعلهم يشعرون بمزيدٍ من المساواة عملياً (حيث ستتاح لهم المنصات الأساسية والمعلومات والموارد الشبكية نفسها) بينما ستبقى الفروقات الأساسية في العالم المادي. وإذا كانت الاتصالات لن تحل مشكلة اللامساواة في الدخل، فإنها ستخفف من بعض أسبابها ونتائجها المزمنة؛ كالنقص في الفرص التعليمية الاقتصادية المتاحة. لذا، علينا أن نعترف بالابتكار ونحتفي به ضمن سياقه، فالجميع سينتفعون من الاتصالات؛ لكن ليس على قدم المساواة. وسيكون تركيزنا هنا على تجليات هذه الفروقات في الحياة اليومية للناس.

تحسن الفعالية

بفضل قدرتنا على فعل المزيد في العالم الافتراضي تصبح آليات عالمنا المادي أكثر فعالية. فمع وصول الاتصالات الرقمية إلى أقاصي المعمورة سيستخدمها مستخدمون جدد لتحسين طيفٍ واسعٍ من الأسواق والنظم والسلوكيات غير الفعالة في المجتمعات الأكثر تقدماً والأقل تقدماً. وستكون المكاسب الناتجة عن ذلك في مجال الفعالية والإنتاجية كبيرة؛ وخاصة في الدول النامية التي أدت فيها العزلة التقانية والسياسات السيئة إلى كبح النمو والتقدم لسنوات، وحيث سيحقق الناس كثيراً بالقليل.

سيُحدث توفر أجهزةٍ ذكية مقبولة التكلفة من هواتف وحواسب لوحية تحولاً في هذه البلدان. لنر مثلاً أثر أجهزة الهواتف النقالة البسيطة على حياة مجموعةٍ من صيادات السمك في الكونغو اليوم؛ فبينما كنّ معتادات على إحضار صيدهن اليومي إلى السوق ومشاهدته وهو يفسد مع مرور النهار، صرن اليوم يحتفظن به في النهر - بعد أن يعلق في الأشراك التي ينصبنها - حيث يقفن رتلاً وينتظرن اتصالات الزبائن. وعندما تصلهنّ طلبيةٌ، يتم إخراج السمك من الماء وأخذه للشاري. لم تعد هناك حاجةٌ للبرادات المكلفة، ولا لشخصٍ يحرس السمك في الليل، ولم يعد خطر فساد السمك وخسارته قيمته (أو تسميمه الزبائن) قائماً، ولم تعد هناك حاجةٌ

للصيد الزائد، بل يمكن لحجم سوق النساء هذه أن يزداد أكثر بعد عبر التنسيق مع صيادي السمك في المناطق المحيطة باستخدام هواتفهن الخاصة. وكبديلٍ عن اقتصاد السوق الرسمي (الذي قد يتطلب تطويره سنوات) ليس هذا الحل الالتفافي سيئاً بالنسبة إلى النساء أو بالنسبة إلى المجتمع بشكلٍ عام.

تحدث الهواتف النقالة تحولاً في طريقة وصول الناس في العالم الثالث إلى المعلومات واستخدامهم لها. وهي تنتشر بمعدلاتٍ لا تنفك ترتفع. فاليوم، يوجد في أفريقيا نحو 650 مليون مستخدم هاتف نقال، وما يقارب ثلاثة مليارات في أنحاء آسيا. ويستخدم معظم هؤلاء الميزات الأساسية للهاتف فقط - من اتصالاتٍ صوتية ورسائل نصيّة - لأن تكاليف خدمات البيانات في بلدانهم غالباً ما تكون مرتفعة إلى حدٍّ تعجيزي؛ حتى إن أولئك القادرين على شراء هواتف ذكية أو أية هواتف تحمل ميزة الوب لا يستطيعون استخدامها نتيجةً لارتفاع تكلفة الوب. لكن ذلك سيتغير. وعندما يحدث ذلك، ستقدم ثورة الهاتف الذكي منافع حاسمة لهذه الشعوب.

يعيش مئات الملايين من الناس اليوم الحياة التي عاشها أجدادهم في بلدانٍ لا يتجاوز متوسط العمر المتوقع فيها الستين عاماً أو حتى الخمسين في بعض الأماكن. وما من شيء يضمن أن يطرأ تحسنٌ جذري على ظروفهم السياسية والمايكرواقتصادية في أي وقت قريب. لكن الجديد في حياتهم وفي مستقبلهم هو الاتصالات. ومن المهم هنا تواجد فرصة أمامهم لتجاوز التقانات الأكثر قدماً، كمودمات الطلب الهاتفي، والانتقال مباشرةً إلى الاتصالات اللاسلكية عالية السرعة؛ مما يعني أن التحولات التي سترافق الاتصالات ستحدث بسرعةٍ أكبر مقارنة بما حدث في العالم المتقدم. والتحولات التي يحدثها دخول الهواتف النقالة أكبر بكثير مما يمكن لمعظم الناس في البلدان المتقدمة أن يدركوه. فمع اتصال الناس بالشبكة يصبحون فجأةً قادرين على الوصول إلى معظم معلومات العالم بلغتهم الخاصة أينما كانوا في أنحاء العالم. وينطبق ذلك على راعي قطيع أمي من الماساي في سيرنغري، رغم أن لغته الأم - لغة الما - ليست مكتوبة، حيث يمكنه أن يستفسر شفهياً عن أسعار السوق لليوم، وأن يجمع معلومات من عامة الناس عن أماكن تواجد الحيوانات المفترسة في الجوار، ليأتيه الجواب منطوقاً من جهازه. ستسمح الهواتف الخلوية للناس الذين كانوا معزولين في السابق بالتواصل مع أشخاصٍ آخرين بعيدين عنهم جداً ومختلفين عنهم جداً. أما على الجبهة الاقتصادية، فإنهم سيجدون طرقاً يستغلون بها الأدوات الجديدة المتاحة بين أيديهم لتوسيع أعمالهم وزيادة فعاليتها، ولزيادة أرباحهم؛ كما فعلت صيادات السمك بفضل هواتفهنّ النقالة البسيطة.

بعيداً عن الهواتف النقالة، إنّ ما تقدمه الاتصالات أيضاً هو القدرة على جمع البيانات واستخدامها. البيانات بحدّ ذاتها أداة، ففي الأماكن التي تقف فيها الإحصاءات غير الموثوقة حول الصحة والتعليم والاقتصاد وحاجات السكان عائقاً أمام النمو والتطور، من شأن إمكانية جمع البيانات بطريقة فعالة تغيير قواعد اللعبة. فالجميع في المجتمع يستفيدون من البيانات الرقمية، حيث يمكن للحكومات استخدامها لقياس مدى نجاح برامجها، بينما تستخدمها وسائل الإعلام

وغيرها من المنظمات غير الحكومية لدعم عملها وللتوثق من المعطيات. فبإمكان موقع أمازون على سبيل المثال أن يستخدم بيانات التجار المتوفرة لديه ويطبق عليها خوارزميات تقوم بتطوير قروض مصرفية مخصصة تعرض على هؤلاء؛ وقد يتم ذلك في حالات تغلق فيها المصارف التقليدية أبوابها بالكامل. ويمكن عبر بناء أسواق أكبر وتطبيق معايير أفضل الوصول إلى اقتصادات أكثر صحة وإنتاجية.

لن يبقى العالم النامي في معزل عن هذه التطورات التي تحدث في مجال المعدات والآلات عالية التقنية الأخرى. فحتى إذا كانت أسعار الهواتف الذكية المتطورة والروبوتات التي تقوم بالأعمال المنـزلية - كالتنظيف بالمكنسة الكهربائية - مرتفعةً، فإن شبكة مثل شانـزهاي للكهربائيات في الصين ستنتج وتوسع وتوزع منتجاتٍ مقلدةٍ تردم هذه الهوة. وستجد التقانات التي ظهرت في سياقات العالم الأول أهدافاً جديدةً لها في البلدان النامية. فمن خلال التصنيع المضاف، أو الطباعة ثلاثية الأبعاد، يمكن للآلات بالفعل طباعة مجسمات أو أغراض مادية؛ حيث تستقبل بيانات ثلاثية الأبعاد عن غرض ما، وتتتبّع الحدود المحددة لشكله لتكوِّنه على طبقاتٍ فائقة الرقة، طبقةً تلو الأخرى، بواسطة بلاستيك سائل أو مادةٍ أخرى حتى يتجسد الغرض كاملاً. لقد قامت مثل هذه الطابعات بإنتاج طيف واسع من الأغراض كالهواتف النقالة المخصصة، وقطع الغيار، والدراجات النارية المنسوخة بالحجم الطبيعي. وسيكون لهذه الآلات بكل تأكيد أثرها في العالم النامي؛ حيث سيتمكن الناس في البلدان الفقيرة من تصنيع أية أداةٍ أو قطعةٍ يحتاجون إليها باستخدام طابعاتٍ ثلاثية الأبعاد خاصة باستخدام قوالب مفتوحة المصدر (أي معلومات رقمية متوفرة مجاناً مع مصادرها القابلة للتحرير) بدلاً من انتظار وصول بضائع جاهزة مرتفعة الأسعار عبر طرق توصيل طويلة ومتعبة ومقيدة بشروط.

أما في البلدان الأغنى، فإن الطباعة ثلاثية الأبعاد ستكون الشريك الأفضل للتصنيع المتقدم، فسيتم بناء المواد والمنتجات الجديدة بالكامل بشكلٍ مخصص، وفقاً لمواصفات تأتي عبر الإنترنت تنفذها عند الطلب آلة يشرف عليها شخص محترف ومدَّرب. ولن يكون ذلك بديلاً عن تلك الهكتارات من المرافق الصناعية عالية الإنتاج ومنخفضة التكلفة الموجودة في الكثير من الصناعات، لكنه سيقدم تنوعاً غير مسبوق في المنتجات المستخدمة في العالم النامي.

أما في ما يتعلق بالمهام اليومية الصغيرة في الحياة، فستساعد نظم المعلومات على إيكال الكثير منها إلى أناسٍ يعيشون في هذه البلدان؛ كآلات الملابس المتكاملة (التي تقوم بالغسيل والتجفيف والطوي والضغط والفرز) التي تحتفظ بمخزون من الملابس النظيفة، وتطبق خوارزميات لاقتراح الملابس المناسبة وفقاً للبرنامج اليومي للمستخدم. وستتم أخيراً أتمتة حلاقة الشعر لتصبح عملية آلية محكمة. وستكون للهواتف الخلوية والحواسب اللوحية والمحمولة القدرة على الشحن لاسلكياً؛ بما يجعل الحاجة إلى الأسلاك واحداً من إزعاجات الماضي. ومع مركزة الكثير من الأجزاء المتحركة في حياتنا ضمن نظام إدارة معلومات واتخاذ قرارات سهل الاستخدام وشبه بديهي، سنشعر بأن تفاعلنا مع التقانة لا يكلفنا أي

عناء. وطالما اتخذت الإجراءات الاحترازية التي تحافظ على خصوصيتنا وتحمي بياناتنا من الضياع، فإن هذه النظم ستحررنا من الكثير من الأعباء الصغيرة (كالمراسلات الشفهية، ولوائح المهام، ومهام "المراقبة" المتنوعة) التي تسبب لنا الضغط، وتقتطع من تركيزنا الذهني خلال النهار. ستساعد نظم المعلومات المصممة لتلبية احتياجاتنا على إكمال محدودياتنا العصبية التي تؤدي بنا إلى السهو والإغفال. وثمة مثالان على هذه النظم هما الذاكرة البديلة (تذكيرات التقويم ولوائح المهام)، والعضوية الاجتماعية البديلة التي تصلك لحظياً بصديق لديه خبرة ذات صلة بأية مهمة بين يديك.

باعتمادنا على هذه الأنظمة المتكاملة التي تجمع الوجهين؛ المهني والشخصي في حياتنا، سيصبح بوسعنا استغلال وقتنا يومياً بمزيد من الفعالية؛ بما يعنيه ذلك من توفر المزيد من الوقت لدينا، سواء أستفدنا منه للتفكير العميق أم للتحضير لعرض تقديمي هام أم لضمان أن يتمكن أب من حضور مباراة كرة قدم يشارك فيها ولده من دون أن يشغله عن ذلك شيء. وستكون محركات الاقتراح - التي تقترح مفردات بديلة لمساعدة المستخدم على إيجاد ما يبحث عنه - مفيدة على نحو خاص في تحقيق الفعالية عبر محاكاتها المستمرة لعمليات التفكير لدينا؛ حيث ينتهي بها المطاف إلى زيادة إبداعنا وليس إلى الاستحواذ عليه. وسيكون العالم بالطبع مليئاً بالأدوات وإمكانيات الرسوم المجسمة التي تسمح لنسخة افتراضية منك بأن تتواجد في مكان آخر، مع مقادير لانهائية من البيانات، حيث تكون هناك طرق كثيرة للمماطلة أيضاً، لكن الفكرة من وراء ذلك هي أنك إذا اخترت أن تكون منتجاً، فيمكنك أن تكون كذلك بقدرة مضاعفة.

ثمة أمور أخرى أوشكت على النضوج في مجالات مثل الروبوتات، والذكاء الصناعي، والتعرف على الصوت ستدخِل مزيداً من الفعالية إلى حياتنا؛ عبر توفير المزيد من أشكال التفاعل السلس مع التقانة في روتيناتنا اليومية. وإذا كانت الروبوتات الآلية بالكامل الشبيهة بالبشر والمزودة بقدرات ذكاء صنعي مذهلة ستبقى خارج القدرة الشرائية لمعظم الناس لبعض الوقت، فإن المستهلك الأمريكي العادي سيجد نفسه في وقت قريب جداً قادراً على اقتناء مجموعة منوعة من الروبوتات متعددة الأهداف. فالتقانة المستخدمة في مكنسة رومبا الكهربائية من إنتاج آي. روبوت - وهي من النماذج المبكرة في ميدان روبوتات المستهلك "المنـزلية" (حيث ظهرت أولاها عام 2002) - لن تنفك تتطور مع الوقت وتتعدد استخداماتها. ويفترض أن تكون النماذج المستقبلية قادرة على تولي الواجبات المنـزلية الأخرى، والأعمال الكهربائية، بل وحتى مشكلات السمكرة، بسهولة نسبياً.

يجدر بنا أيضاً أن لا نغفل الأثر الذي ستتركه البرمجيات المتفوقة للتعرف على الصوت على حياتنا اليومية. فبعيداً عن البحث عن المعلومات على الإنترنت صوتياً وإصدار الأوامر إلى روبوتاتك (وكلاهما ممكنان اليوم)، سيؤدي تحسن التعرف على الصوت إلى إمكانية التحويل اللحظي لكل ما تنتجه إلى نص، من البريد الإلكتروني إلى الملاحظات والخطابات والأبحاث الجامعية. وبما أن معظم الناس يتكلمون

أسرع مما ينضدون، فإنه لا شك في أن هذه التقانة ستوفر وقت الكثيرين منا في شؤونهم اليومية، ناهيك عن مساعدتها لنا على تجنب حالات متلازمة النفق الرسغي. كما أن التحول إلى الكتابة عن طريق الكلام من شأنه أن يغير عالم المادة الكتابية الذي نعيش فيه. فهل سنتعلم الكلام في فقرات؟ أم إن كتابتنا ستبدأ بمحاكاة نماذج الكلام الشفاهي لدينا؟

لقد أصبح الاستخدام اليومي لتقانة التعرف على الإيماءات أقرب مما نعتقد. فقد حقق جهاز كِنيكت من مايكروسوفت - وهو جهاز حساس لا يحتاج إلى استعمال اليدين، يستخدم لمنصة ألعاب الفيديو إكس. بوكس 360 فيلتقط حركة اللاعب ويوظفها - رقماً قياسياً عالمياً عام 2011 كأسرع إلكترونيات المستهلك مبيعاً في التاريخ؛ حين بيع منه أكثر من ثمانية ملايين جهاز في أيامه الستة الأولى في السوق. ولن يمر وقت طويل حتى تخرج الواجهات الإيمائية من إطار الألعاب والترفيه لتدخل ميادين أكثر وظيفية. فواجهات المعلومات المستقبلية التي كانت معروضة بشكل بارز في فيلم تقرير الأقلية الذي استخدم فيه توم كروز تقانة الإيماء والصور المجسمة لحلّ لغز الجرائم على الحاسب، ليست سوى البداية. بل إننا قد تجاوزنا ذلك بالفعل، فالعمل المشوق حقاً اليوم هو بناء "روبوتات اجتماعية" قادرة على فهم إيماءات الإنسان والاستجابة لها وفقاً لنوعها، مثل دمية كلب تجلس حين يقوم طفل بإيماءة آمرة.

كما أننا، إذا تابعنا سبرنا لهذا الرتل، فقد لا نحتاج إلى الحركة المادية لكي نتعامل مع هذه الروبوتات. فقد تحققت سلسلة من التطورات المثيرة في تقانة الحركة التي يتم التحكم بها بمجرد التفكير - أي التحريك مباشرة عبر التفكير فقط - خلال السنوات القليلة الأخيرة. ففي عام 2012، قدم فريق في مخبر للروبوتات في اليابان عرضاً ناجحاً لشخص مستلقٍ في آلة تصوير بالرنين المغناطيسي الوظيفي (التي تجري مسوحات مستمرة للدماغ لقياس التغيرات في دفق الدم) استطاع أن يتحكم بروبوت على بعد مئات الأميال بمجرد تخيله تحريك أجزاء مختلفة من جسمه. وكان الشخص في التجربة قادراً على الرؤية بعيني الروبوت بفضل كاميرا مثبتة على رأس الأخير، وعندما كان يفكر في تحريك ذراعه أو ساقيه، كان الروبوت يتحرك بطريقة مماثلة وبشكل شبه لحظي. فالإمكانيات التي تطرحها الحركة التي يتم التحكم بها بمجرد التفكير - ليس فقط على شكل روبوت مستقل أشبه بالوكيل، بل أيضاً في مجال الأطراف الاصطناعية - ستكون مثيرة بشكل خاص لما تبشر به الأفراد ذوي الصعوبات الحركية أو أولئك المقعدين؛ مثل مرضى إصابات النخاع الشوكي، وذوي الأطراف المبتورة، وغيرهم ممن لا يستطيعون التواصل أو الانتقال نتيجة حالتهم الجسدية الراهنة.

المزيد من الابتكار، يعني المزيد من الفرص

لن يكون مفاجئاً أن تحافظ مسيرة العولمة الثابتة على زخمها، بل وأن تتسارع مع انتشار الاتصالات. لكن ما قد يفاجئك هو كيف سيبدو عالمك صغيراً مع التقدمات التقانية المصحوبة بزيادة في الاتصالات وفي الاعتمادية البينية بين الدول. فالترجمة

الفورية وتفاعلات العالم الافتراضي والتحرير التعاوني بالزمن الحقيقي - وأبسط أشكاله المعروفة اليوم هو مدونات الويكي - ستغير كلها طريقة تفاعل الشركات والمنظمات مع الشركاء والزبائن والموظفين في أماكن تواجدهم. ومع أن بعض الفروقات قد لا يتم التغلب عليها أبداً، مثل الفوارق الثقافية والمناطق الزمنية، إلاّ أنّ القدرة على التفاعل مع البشر في أماكن متفاوتة، مع قدرة شبه كاملة على الفهم على منصات مشتركة ستجعل هذه التفاعلات تبدو طبيعية على نحو لا يصدق.

ستصبح سلاسل الإمداد الخاصة بالمؤسسات التجارية وغيرها من المنظمات مستقلة باضطراد، ليس فقط من ناحية الإنتاج، بل أيضاً في ما يتعلق بالبشر. فازدياد فعالية الاتصالات العابرة للحدود واللغات سيؤدي إلى بناء الثقة وتوليد الفرص للأفراد النشيطين والموهوبين حول العالم. ولن يكون من الغريب أن تشغّل شركة تقانة فرنسية فريق مبيعاتها في جنوب شرق آسيا، بينما توزع مسؤولي الموارد البشرية في كندا والمهندسين في مصر. أما العوائق البيروقراطية التي تمنع هذا المستوى من التشغيل اللامركزي اليوم - كقيود تأشيرات الدخول والقوانين المتعلقة بتحويل الأموال - فستصبح غير ذات صلة، أو سيتم التغلب عليها مع اكتشاف حلول رقمية. فربما تقوم منظمة حقوق إنسان يعيش كوادرها في بلد فرضت عليه عقوبات دبلوماسية بتسديد رواتب موظفيها بواسطة أرصدة المال سهل الانتقال، أو باستخدام عملة رقمية تماماً.

مع انحسار فرص العمل التي تتطلب حضوراً شخصياً، سيتاح للموهوبين المزيد من الخيارات. وسيجد الشباب المؤهلون في هنغاريا أنفسهم في منافسة مع أقرانهم من بلاد البرتقال (كاليفورنيا) على أنواع معينة من فرص العمل. وكما أنه ليس كل عمل قابلاً للأتمتة في المستقبل، أو لا يراد له ذلك، فليس كل عمل قابلاً للإنجاز عن بعد. لكن الأعمال القابلة لذلك أكثر مما تعتقد. وسيجد أولئك الذين يعيشون على بضعة دولارات في اليوم فرصاً لا حد لها تتيح لهم تحسين مدخولهم. وبالفعل، فإن خدمة ميكانيكال تورك من أمازون، وهي منصة رقمية لتوزيع المهام، تقدم لنا مثالاً من الحاضر للشركة التي تعهد بمهام صغيرة يمكن إنجازها لقاء بضعة سنتات إلى أي شخص يتوفر لديه اتصال إنترنت. ومع استمرار تحسن جودة التفاعلات الافتراضية، قد تتوسع قاعدة زبائن المنصة بطيف واسع من المهن، فقد تتعامل مع محامٍ من قارة ما وتستخدم وسيطاً عقارياً من قارة أخرى. وقد يستنكر نقاد العولمة هذا التآكل للاحتكارات المحلية، لكن لا بد لهم من قبوله، فهكذا ستسير مجتمعاتنا قدماً، وهكذا ستستمر في الابتكار. إن نهضة الاتصالات يجب أن تساعد البلدان بالفعل على استكشاف ميزاتها التنافسية، فربما كان أفضل المصممين الرسوميين في العالم من بوتسوانا، وكل ما في الأمر هو أن العالم يجهل ذلك حتى الآن.

ستمتد عملية تسوية ميدان المنافسة إلى عالم الأفكار، وسيزداد ظهور الابتكار من الهوامش بعيداً عن المعاقل التقليدية للنمو؛ مع شروع الناس بإقامة اتصالات جديدة وتناول مشكلات صعبة من وجهات نظر فريدة بما يدفع التغيير قدماً. ستضمن المستويات الجديدة من التعاون والتلقيح المتبادل بين مختلف القطاعات

إتاحة الفرصة لبروز الكثير من أفضل الأفكار والحلول التي ستخضع للنظر والتقييم والاستكشاف ويتم تبنيها وتمويلها والاحتفاء بها. فربما يكتشف مبرمج روسي طموح يعمل حالياً مدرساً في نوفوسيبيرسك تطبيقاً جديداً للتقانة القائمة وراء لعبة أنغري بيردز؛ حيث يدرك أن إطار العمل المستخدم في اللعبة يمكن استخدامه لتحسين الأدوات التعليمية التي يقوم ببنائها لتدريس الفيزياء للتلاميذ المحليين. فيعثر على برمجيات ألعاب مشابهة مفتوحة المصدر ويشرع بالبناء عليها. ومع ازدياد زخم حركة المصدر المفتوح في العالم (فهي رخيصة الكلفة بالنسبة إلى الحكومات والشركات، بينما تتمثل منافعها بالنسبة إلى المساهمين في التقدير الذي يحظون به، وبالفرص الاقتصادية التي توفرها، والتي تحسّن النظم البيئية الداعمة وتوسّعها)، ستتوفر لدى المبرمج - المدرّس الروسي ذخيرة هائلة من الخطط التقنية يتعلم منها ويستخدمها في عمله الخاص. وسيكون من المحتمل جداً في عالم مترابط بالكامل أن يلفت نظر الأشخاص المناسبين، فتعرض عليه فرص عمل أو منح دراسية، أو قد يبيع ابتكاراته لشركة كبرى متعددة الجنسيات. لكنه على الأقل سيحظى بفرصته.

ربما يأتي الابتكار من القاعدة، لكنْ لن يكون كل ابتكار محلي مؤهلاً للنجاح على مستوى أعلى، فبعض المقاولين والمخترعين سيكونون منكبين على البناء لجمهور مختلف، وعلى حل مشكلات على قدر كبير من الخصوصية؛ وهو ما نشهده اليوم بالفعل. فقد كشف المخترع الكيني أنطوني موتوا الذي يبلغ من العمر أربعة وعشرين عاماً في معرض علمي في نيروبـي عن شريحة كريستال فائقة الرقة قام بتطويرها قادرة على توليد الكهرباء عندما توضع تحت ضغط. فوضع الشريحة على كعب حذاء تنس، وعرض كيفية تمكن المرء من شحن جهازه النقال بمجرد السير. (إن قيام مبتكرين من أمثال موتوا بتصميم رقائق صغرية تحول الأفراد إلى محطات شحن متنقلة إنما يذكر بمدى الإزعاج الذي تسببه مشاكل توفر الكهرباء وأسعارها لكثير من الناس، وكذلك قصر عمر البطاريات وإنما بقدر أقل، وبتقاعس الحكومات عن إصلاح شبكات الكهرباء). لقد هُيئت شريحته الآن لتدخل الإنتاج الكمي. وإذا أدى ذلك إلى تخفيض تكلفة الإنتاج بنجاح فسيكون موتوا قد اخترع واحداً من أذكى التصاميم التي لن يستخدمها أحد خارج العالم النامي؛ ببساطة لأن لا أحد هناك يحتاج إليها. لكن مستوى توفر التقانة للناس غالباً ما يكون محكوماً بعوامل خارجية للأسف، فحتى إذا حُلت مشكلات الطاقة والكهرباء في النهاية (سواء أتمّ ذلك على أيدي الحكومات أم على أيدي المواطنين)، فإننا لا نعرف بعد العقبات التي قد تمنع مجموعات معينة من الوصول إلى مستوى التواصل نفسه والمقدار نفسه من الفرص الذي ستصل إليه مجموعات أخرى.

ستشهد أهم الركائز التي يقوم عليها الابتكار والفرص التي ترافقه، أي التعليم، تغيرات إيجابية هائلة في العقود القادمة؛ مع إعادة صياغة إجراءاتنا التقليدية بفضل تصاعد الاتصالات بما يطرح مساراتٍ جديدة للتعلم. فسيكون معظم الطلاب على قدرٍ عالٍ من التأهيل التقاني مع استمرار المدارس في مكاملة التقانة في خططها التدريسية واستبدالها في بعض الحالات بالدروس التقليدية مع مزيدٍ من ورشات

العمل التفاعلية. وسيصبح التعليم تجربةً أكثر مرونة تتأقلم مع أساليب تعلم الأطفال وسرعتهم في التعلم بدلاً من أن يحدث العكس. وسيستمر الأطفال الصغار في الذهاب إلى المدرسة من أجل النشاط الاجتماعي والحصول على إرشادات المعلمين، لكن قدراً مماثلاً أو ربما أكبر من عملية التعلم سيتم عن طريق تطبيق أدوات تعليمية مصممة بعناية وتقلد روحية أكاديمية خان؛ وهي منظمةٌ غير ربحية تنتج الآلاف من مقاطع الفيديو القصيرة (معظمها في العلوم والرياضيات) وتشاركها مجاناً على الإنترنت. وتبين مئات الملايين من المشاهدات على قناة أكاديمية خان على اليوتيوب أن اعتماد الأساتذة في الولايات المتحدة عليها لا ينفك يزداد باضطراد. وهم يدمجون أسلوب مؤسسها سلمان خان المتمثل في التعلم ضمنَ وحدات مفصلة لحاجات الطالب. بل إن بعضهم يقومون بقلب حصصهم الدراسية مستبدلين المحاضرات بمشاهدة الفيديو في المنـزل كوظيفة، واستخدام الوقت في المدرسة لإنجاز الوظائف المنـزلية التقليدية مثل حل مجموعة من المسائل في حصة الرياضيات. وستصبح مهارات التفكير النقدي وحل المشكلات محور اهتمام الكثير من نظم المدارس مع انتشار أدوات المعرفة الرقمية في كل مكان، مثل المقاطع الأكثر دقة في الويكيبيديا حيث تخفف من دور الحفظ عن ظهر قلب.

أما بالنسبة إلى الأطفال في البلدان الفقيرة، فإن الاتصالات المستقبلية تَعِد بإتاحة أدواتٍ تعليميةٍ جديدة؛ وإن لم تكن بمستوى تلك الموصوفة أعلاه تماماً. وستُهجر القاعات الدراسية، لكن المعلمين سيستمرون في تلقي رواتبهم من دون أن يحضروا إلى الصفوف. وستصبح الكتب والتجهيزات نادرةً، لكن المتحول الجديد في هذه المعادلة، أي الاتصالات، يعد بإتاحة الأجهزة النقالة للأطفال وكذلك الإنترنت؛ ممّا يمكنهم من ممارسة الحياة المدرسية جسدياً وافتراضياً، وإن كانت الأخيرة غير رسمية ويمارسونها في وقتهم الخاص.

في الأماكن التي لا تلبـي فيها الحكومات الحاجات الأساسية على نحو لائق، وفي المناطق غير الآمنة، ستمثل التقانات الرقمية الأساسية، كالهواتف النقالة، بدائل آمنة ورخيصة للعائلات التي تتطلع لتعليم أولادها. وسيكون أمام الطفل الذي لا يستطيع الذهاب إلى المدرسة - بسبب المسافة أو غياب الأمن أو بسبب ارتفاع رسوم الدراسة فيها - طوق نجاة يوصله إلى عالم التعليم؛ إذا كان بين يديه هاتف نقال. وحتى إنّ الأطفال الذين لا تتاح لديهم شبكات البيانات أو الوب النقال ستُوفر لهم الخدمات النقالة الأساسية؛ كالتراسل النصي، وخدمة المجيب الصوتي التفاعلي (وهو شكل من أشكال تقانة التعرف على الصوت)، ومنافذ تعليمية. وإذا تم تجهيز الحواسب اللوحية والهواتف النقالة قبل بيعها بتطبيقات تعليمية عالية الجودة وبمحتويات ترفيهية، فإن ذلك سيضمن أن يستفيد من توفر هذه الأجهزة ذوو "عرض الحزمة الفقير" الذين لا تتوافر لديهم الاتصالات الموثوقة. وستُتَمِّم هذه الأجهزة النقالة عملية تعليم الأطفال الذين تعاني مدارسهم من الاكتظاظ أو من نقص في الكوادر، أو الذين يكون منهاجهم التعليمي الوطني محدوداً وغير موثوق؛ مما سيساعدهم على استغلال كامل إمكانياتهم بغض النظر عن منشئهم. واليوم

ثمة الكثير من المشاريع التجريبية في البلدان النامية التي تسعى إلى تفعيل التقانة النقالة لتدريس طيف واسع من المواضيع والمهارات، بما فيها التعليم الأساسي للأطفال والكبار، واللغات الثانية، والمناهج المتقدمة في الجامعات. وقد اختبر مخبر الوسائط في معهد ماساشوسيتس للتقانة هذه الطريقة في أثيوبيا عبر توزيع حواسب لوحية محملة مسبقاً بالمحتويات على أطفال المرحلة الابتدائية من دون إعطائهم أية تعليمات، ومن دون مدرسين مرافقين، وكانت النتائج رائعة. فخلال بضعة أشهر حفظ الأطفال الأبجدية كاملةً، وغدوا قادرين على كتابة جمل كاملة باللغة الإنكليزية. ومن دون الاتصالات التي ستكون متوفرةً في كل مكان في المستقبل، تبقى هناك قيودٌ على ما يمكن لأي من هذه المحاولات تحقيقه اليوم.

تخيل فقط ما يمكن أن يحدثه تنامي منصات التعليم المعتمدة على الهواتف النقالة والحواسب اللوحية هذه من آثارٍ في بلدٍ مثل أفغانستان يعاني من أدنى مستويات التعليم في العالم. ستكون مثل تلك المنصات الرقمية، سواء أقُدِّمت في شكل نقال بسيط أم عبر طرقٍ أكثر تعقيداً على الإنترنت، قادرةً في النهاية على مقاومة أية اضطرابات بيئية (سواء أكانت تقلباتٍ سياسية أم انهيارات اقتصادية أو حالاتٍ جوية سيئة)، وستواظب على تخديم مستخدميها. وهكذا، بينما ستبقى العملية التعليمية في العالم المادي غير مستقرةٍ بالنسبة إلى كثيرين، ستصبح التجربة الافتراضية مع الوقت الخيار الأهم والأضمن عاقبةً، وسيجد الطلاب المتورطون في نظم مدرسية تقدم مناهج محدودة أو تعتمد على الحفظ عن ظهر قلب أمامهم عالماً افتراضياً يشجع على الاستكشاف الذاتي والتفكير النقدي.

حياة ذات نوعية أفضل

بالتوازي مع الطيف الواسع من التحسينات الوظيفية على حياتك اليومية، تعد الاتصالات في المستقبل بمجموعةٍ مدهشة من التحسينات المتعلقة بجودة الحياة، وهي أشياء تجعلكِ أكثر صحةً وأمناً ونشاطاً. وكما هو حال المكاسب الأخرى، سيبقى هناك دائماً مقياس متدرج لمدى توفر هذه التحسينات، لكن ذلك لا ينتقص من أهميتها على الإطلاق.

في المستقبل، ستكون للأجهزة والشاشات ومختلف الآلات في شقتك غايات تتجاوز مجرد المنفعة، فهي ستقدم لك الترفيه والتسلية المطلوبة والإغناء الفكري والثقافي والاسترخاء وفرص التشارك مع الآخرين. وسيكون التقدم الأساسي هو إضفاء الطابع الشخصي؛ فسيكون بإمكانك تخصيص أجهزتك، بل ومعظم ما يحيط بك من تقانة؛ حيث تتناسب مع احتياجاتك بما يجعل بيئتك تعكس تفضيلاتك. وستتوفر للناس طرق أفضل يروون بها قصص حياتهم، من دون أن يتوجب عليهم الاعتماد على ألبومات الصور المادية أو الشبكية، علماً أن كلا الخيارين سيبقيان متاحين. وستسمح لك تقانة الفيديو والتصوير الضوئي في المستقبل بتجسيم أية صورة ثابتة أو متحركة تلتقطها لتتخذ شكل مجسم هولوغرافي ثلاثي الأبعاد. والأروع من ذلك أنه سيكون بإمكانك أن تكامل أية إعدادات صور أو فيديو أو إعدادات جغرافية لديك وتحفظها في جهاز هولوغراف واحد يوضع على أرض غرفة

المعيشة لديك ليحول المكان إلى غرفة للذاكرة. وسيستطيع زوجان أن يعيدا إحياء حفل عرسهما ليشاهده جداهما اللذان منعهما المرض من حضوره.

ستكون أنت من يحدد ما يمكنك مشاهدته على مختلف الشاشات التي لديك (سواء أكانت شاشات كريستال سائل - أل.سي.دي - عالية الجودة، أم أجهزة إسقاط هولوغرافية، أم أجهزة نقالة بحجم الكف)، من دون أن تملي عليك برامج التلفزة الشبكية ذلك. وستكون طوع بنانك ثروة عالمية من المحتوى الرقمي الذي يتم تحديثه وتقييمه وتصنيفه على الدوام بما يساعدك على العثور على ما تهواه من الموسيقى والأفلام والبرامج والكتب والمجلات والمدونات والفنون. وستصبح السلطة التي يمارسها الأفراد على قنوات المعلومات والترفيه أقوى من أي وقت مضى مع تحول المنتجين من الإنتاجية المقسمة إلى نماذج أكثر وحدة وانفتاحاً نتيجة للحاجة إلى نموذج تجاري مختلف للحفاظ على الجمهور. ويمكننا منذ الآن أن نستشعر ما سيبدو عليه المستقبل عبر خدمات معاصرة مثل خدمة سبوتيفاي التي تتيح لائحة ضخمة من الموسيقى الحية مجاناً؛ إذ إنّ قدراً غير نهائي من المحتوى متوفر للمستخدمين في أي وقت وعلى أي جهاز تقريباً، وبكلفة لا تذكر أو من دون كلفة؛ مع الحفاظ على حقوق الملكية وسبل العوائد. وستنـزاح العوائق القديمة التي كانت تقف أمام دخول مبدعي المحتوى، فتماماً كما يمكن القول إن يوتيوب يسمح بالانطلاق في مسيرة مهنية اليوم* (أو إنه يوفر بعض الشهرة العابرة على الأقل)، سيتوفر في المستقبل المزيد من المنصات التي تتيح للفنانين والكتّاب والمخرجين والموسيقيين وغيرهم في جميع البلدان فرصة الوصول إلى جمهور أعرض. وسيبقى من الضروري امتلاك المهارة لإنتاج محتوى ذي جودة، لكن تشكيل فريق يحمل المؤهلات المطلوبة سيكون أسهل أيضاً، كأن يعمل رسام رسوم متحركة من جنوب كوريا مع مؤدي صوت من الفلبين مع مؤلف مشاهد من المكسيك وموسيقي من كينيا. وستكون أمام المنتج المنجز فرصة للوصول إلى جمهور عريض؛ تماماً مثل أي فيلم هوليودي رائج.

في المستقبل، سيصبح الترفيه تجربة تغمرك بشكل أكبر، وقابلة للتخصيص على نحو شخصي. وستجعل المرفقات الترويجية المتكاملة من العمليات المتبعة اليوم عمليات سلبية ومملة. فإذا صدف خلال مشاهدتك عرضاً تلفزيونياً أن رأيت سترة ترغب بها أو طبقاً تود تحضيره، فستجد المعلومات المتعلقة بطريقة التحضير أو تفاصيل الشراء متوفرة مسبقاً، إضافة إلى جميع المعلومات الأخرى المتعلقة بالعرض التلفزيوني وحبكته وممثليه ومواقع تصويره. وإذا شعرت بالملل ورغبت في تمضية إجازة لمدة ساعة واحدة، فلمَ لا تشغل صندوق المجسام الهولوغرافي holograph box لتزور كرنفال ريو؟ هل تشعر بالضغط؟ اذهب وأمضِ بعض الوقت على شاطئ في المالديف. هل تخشى أن يصبح أولادك مدللين؟ دعهم يتجولون في حي دارافي الفقير في مومبـي. هل تشعر بالخيبة من تغطية وسائل الإعلام للألعاب الأولمبية المقامة في منطقة زمنية أخرى؟ يمكنك شراء تذكرة هولوغرافية بسعر معقول لتشاهد المنتخب الأولمبـي وهو يتنافس أمام عينيك في نقل حي. سيكون بإمكانك، من خلال الإمكانيات التي تتيحها واجهات الواقع الافتراضي

والإسقاط التجسيمي الهولوغرافي، أن "تشارك" في هذه الفعاليات في أثناء إقامتها لتعيشها وكأنك كنت موجوداً فيها حقاً. وإذا لم يكن هناك شيء يضاهي الشيء الحقيقي، فإن ما سيُقدم لك سيكون شبيهاً بالأصل إلى حدٍّ كبير. وبفضل هذه التقانات الجديدة ستستمتع بالنشاط كما بالاسترخاء أكثر من أي وقت مضى.

سيتوفر لك المزيد من الأمان أيضاً، على الأقل خلال السفر. فبينما لا يزال بعض وسائل النقل الأكثر إثارة، كرحلات الأنبوب فوق - الصوتي Supersonic tube والسفر الفضائي المداري بعيد المنال، بات الانتشار الكلي للسيارات ذاتية القيادة وشيكاً. فقد قطع أسطول غوغل من السيارات ذاتية القيادة الذي بناه فريق من غوغل مع مهندسين من جامعة ستانفورد، مئات الآلاف من الأميال من دون التعرض لحادث، وستنضم نماذج جديدة إلى هذه الرحلة قريباً. وبدلاً من أن تحل محل السائق كلياً، ستكون الخطوة الأولية هي اتباع أسلوب "مساعدة السائق"، حيث يمكن دائماً تشغيل خيار القيادة الآلية؛ تماماً كما يقوم قبطان طائرة بتشغيل الطيار الآلي. وقد أصبحت الجهات الحكومية على اطلاع كامل على الإمكانيات التي تطرحها السيارات ذاتية القيادة، ففي عام 2012 أصبحت نيفادا أول ولاية تصدر تراخيص قيادة للسيارات من دون سائق، ثم صادقت كاليفورنيا على قانونيتها في وقت لاحق من ذلك العام. فتخيل الإمكانيات التي ستتاح من خلال ذلك في مجال قيادة الشاحنات على المسافات الطويلة. إذ بدلاً من تحدي القدرات البيولوجية للسائقين من البشر عبر رحلات تستمر ثلاثين ساعة، يمكن للحاسب أن يتولى المسؤولية الأساسية ليقود الشاحنة لمسافات معينة يستريح السائق خلالها.

ستكون التطورات التي سيشهدها مستقبلنا القريب في مجالي الصحة والطب من أهم التغيرات الثورية الجديدة. وبفضل توسع الاتصالات ستعم الفائدة عدداً أكبر من البشر أكثر من أي وقتٍ مضى في التاريخ. وتبشر التحسنات المتحققة في مجال اكتشاف الأمراض ومعالجتها وإدارة السجلات الطبية ومراقبة الصحة الشخصية بتوفر الرعاية الطبية والمعلومات الصحية على نحوٍ أكثر عدلاً لأعدادٍ من البشر قد تقدر بالمليارات إذا أخذنا بالحسبان سرعة انتشار التقانة الرقمية.

ستصبح القدرات التشخيصية لهاتفك النقال أخباراً قديمة (سيكون بإمكانك بالطبع أن تمسح أعضاء الجسم كما تمسح اليوم الرموز الشريطية للمنتجات). لكنك ستتمكن قريباً من الاستفادة من مجموعة من الإضافات الفيزيائية المصممة لمراقبة صحتك كالروبوتات الميكروسكوبية التي توضع في نظام الدوران لتتتبع ضغط الدم والكشف عن علاّت القلب عند نشوئها والتعرف على السرطانات في مراحلها المبكرة. وداخل الحوض التيتاني الجديد الذي سيركبه جدك، ستكون هناك شريحة قادرة على أداء دور عداد الخطى، وعلى مراقبة مستويات الأنسولين لديه؛ حيث تكتشف السكري في مراحله المبكرة. بل وقد تجري اتصالاً هاتفياً آلياً برقم طوارئ إذا تعرض لسقطة قوية إلى درجة تتطلب الحصول على مساعدة. وسيتوفر لديك نسيج صغري مزروع في الأنف ينبهك لوجود ذيفانات جوية (الذيفان اسم يطلق على كل مادة سامة تنتجها الكائنات الحية) وإلى وجود دلالات على بداية رشح لديك.

سيكون وجود هذه التجهيزات في النهاية بديهياً مثل وجود أدوات المساعدة على المشي الصناعية غير المتحكم بها (التي تمت زراعة نماذجها الأولى في خمسينيات القرن العشرين). فهي توسيعاتٌ منطقية لتطبيقات متابعة الصحة الشخصية التي نراها اليوم، والتي تسمح للناس باستخدام هواتفهم الذكية لتسجيل تمارينهم ومتابعة معدلات الأيض لديهم وتخطيط معدلات الكوليسترول. وقد أصبحت تقانة الصحة الهضمية متوفرةً بالفعل، فقد وافقت إدارة الغذاء والعقارات على أول حبةٍ إلكترونية عام 2012. والحبة التي أنتجتها شركة تعمل في مجال الطب الحيوي تدعى بروتوس ديجيتال هيلث في كاليفورنيا، وتحمل حساساً صغرياً بمساحة ميلمتر مربع واحد، يؤدي الحامض المَعِدي حين يتم ابتلاعها إلى تفعيل الدارة وإرسال إشارة إلى لصاقة صغيرة توضع على الجسم من الخارج (تقوم بدورها بإرسال البيانات إلى هاتفٍ نقال). يمكن لهذه اللصاقة أن تجمع معلومات عن استجابة المريض لعقار ما (عبر مراقبة درجة حرارة الجسم ومعدل نبض القلب وغيرها من المؤشرات)، وأن توجه البيانات المتعلقة بالاستخدام المنتظم إلى الأطباء، بل وأن تراقب ما يتناوله الشخص. وستدخل هذه التقانة تحسينات هامة على حياة أولئك الذين يعانون من أمراض مزمنة والكبار منهم بالتحديد: التذكير الآلي بمواعيد تناول الأدوية، والقدرة على القياس المباشر لتفاعلات العقاقير ضمن جسم المريض، وإقامة حلقة تغذية راجعة رقمية لحظية مع الأطباء تكون مخصصة للمريض ومعتمدة على بياناته. وإن لم يكن كل شخص راغباً بمراقبة صحته على نحو فعال إلى هذا الحد، ناهيك بالنسخة الأكثر تفصيلاً التي ستتاح في المستقبل، فلا شك في أن الجميع سيرغبون بأن يتمكن طبيبهم من الوصول إلى هذه المعلومات. ستكون تكلفة "الحبوب الذكية" والنسج المزروعة في الأنف مقبولة إلى حدٍّ يجعلها متوفرة مثل الفيتامينات والمكملات الغذائية. ولن يمر وقتٌ طويل حتى تتاح لنا نظم رعاية صحية شخصية يتم تشغيلها على أجهزتنا النقالة، وتقوم باكتشاف أية مشكلات نتعرض لها آلياً بناءً على البيانات المجموعة من بعض الإضافات المذكورة آنفاً، فتشير إلينا عارضةً خيارات تحديد موعد مع طبيب قريب لتقوم بعد ذلك (بعد موافقتنا) بإرسال جميع البيانات ذات الصلة حول الأعراض والمؤشرات الصحية إلى الطبيب الذي ستتم استشارته.

سيتمكن مهندسو الأنسجة من زراعة أعضاءٍ جديدة لاستبدال الأعضاء القديمة أو المريضة باستخدام مواد صناعية أو باستخدام خلايا المريض نفسه. وسيكون استخدام هذه الأعضاء محدوداً في البداية نظراً إلى تكاليفها، وستنحسر الطعوم grafts (ويقصد بها هنا الازدراع التعويضي) الاصطناعية للبشرة المتوفرة اليوم مفسحة الطريق لطعومات مصنوعة من خلايا ضحايا الحرائق أنفسهم. أما في المشافي فستتولى الروبوتات* المزيد من المسؤوليات، وسيوكل الجراحون المزيد والمزيد من المهام الصعبة للآلات المتطورة حين يتطلب الأمر عملاً دقيقاً أو مملاً، أو عندما يتطلب العمل مجال حركة أوسع.

ستستهل التطورات في الاختبارات الجينية عصر الطب المخصص على المستوى الشخصي. فعبر الاختبارات الموجهة والتحليل الجيني (أي تفكيك شيفرات

كامل الدي.أن.أيه للشخص) ستتاح للأطباء وللمتخصصين بالآفات معلومات أكثر عن مرضاهم ستساعدهم أكثر من أي وقت مضى. وتبقى الاستجابة السلبية الشديدة لبعض العقارات الموصوفة سبباً رئيساً لدخول المشفى وللوفاة بالرغم من التقدم العلمي المطّرد، لقد اتبعت شركات الأدوية أسلوباً تقليدياً يتمثل في "قياس واحد يناسب الجميع" خلال تطوير الأدوية، لكن ذلك سيتغير مع استمرار تطور مجال الصيدلة الحيوية الذي لا يزال في طور النشوء. فتحسن الاختبارات الجينية سيؤدي إلى تخفيض احتمال الاستجابات السلبية مما يحسن فرص المرضى ويقدم المزيد من البيانات للأطباء والباحثين الطبيين ليقوموا بتحليلها واستخدامها. أخيراً، سيكون من الممكن - للأغنياء فقط في البداية - تركيب عقاقير صيدلانية مفصلة للبنية الجينية للفرد. لكن ذلك سيتغير بدوره حين تنخفض تكاليف تحليل الدي.أن. أيه إلى أقل من مئة دولار، وبعد أن يكون قد تم تحليل كل شيء عضوي تقريباً بما يجعل استفادة عدد أكبر بكثير من سكان العالم من التشخيصات عالية التخصيص والمخصصة للشخص أمراً ممكناً.

أما بالنسبة إلى أولئك الذين يعيشون في البلدان النامية، فإن الاتصالات الأساسية والوصول إلى العالم الافتراضي ستوفر لهم مورداً يمكنهم استغلاله لتحسين جودة حياتهم، وسيتحقق ذلك في مجال الصحة أكثر من أي مجال آخر. فبالرغم من كون بيئاتهم في العالم المادي موصومة بالرعاية السيئة، والنقص في اللقاحات والأدوية، والنظم الصحية الفاسدة، وغيرها من العوامل الخارجية التي تؤدي إلى أزماتٍ صحية (كالهجرة الداخلية المتعلقة بالنـزاعات)، فإن مكاسب هامة في مجال الرعاية الصحية سيتم تحقيقها عبر الاستخدامات المبتكرة للهواتف النقالة، والتي ستأتي معظمها من أفراد ومؤسساتٍ غير حكومية تنتهز الفرصة للمبادرة بالتغيير في نظام كان لولاهم سيبقى راكداً. وهذا ما يمكننا منذ الآن أن نراه وهو يحدث، فعبر أنحاء العالم النامي اليوم كانت ثورة "الصحة النقالة" (أي استخدام الهواتف النقالة كأدوات لوصل المرضى بالأطباء ولمراقبة توزيع العقاقير وزيادة مجال تأثير العيادات الصحية) مسؤولة عن إدخال الكثير من التحسينات؛ مع تعامل الكثير من شركات التقانة الناشئة والمقاولين والمنظمات غير الربحية مع مشكلاتٍ صعبة بتبني حلول مبنية على التقانة في المقام الأول. فالهواتف النقالة تستخدم اليوم لتتبع شحنات العقاقير والتوثق من صحتها، ولمشاركة المعلومات الصحية الأساسية غير المتوفرة محلياً، ولإرسال رسائل التذكير المتعلقة بالأدوية والمواعيد إلى المرضى، ولجمع بيانات المؤشرات الصحية التي يمكن للمسؤولين الحكوميين وللمنظمات غير الحكومية وغيرهم من الفاعلين استخدامها لتصميم برامجهم الصحية. أما المشكلات المركزية في القطاعات الصحية في الأماكن الفقيرة، كنقص الكوادر في العيادات، ونقص الخدمة المقدمة للمرضى في الأماكن البعيدة، والنقص في الأدوية أو عدم كفاية توزيعها، وسوء المعلومات المتعلقة باللقاحات وبالوقاية من الأمراض، فستجد كلها حلولاً جزئية على الأقل من خلال الاتصالات.

إن أقل ما يمكن قوله هنا هو أن الاعتماد على الهواتف النقالة سيمنح الناس

مستوى أعلى من التحكم بصحتهم الشخصية؛ وإن كانت هذه الأجهزة بحدّ ذاتها غير قادرة بالطبع على شفاء الأمراض. لكن الناس سيستخدمون هواتفهم للوصول إلى المعلومات الصحيّة الوقائية أو الشفائية، ويمكنهم استخدام أدوات تشخيص أساسية متوفرة في هواتفهم، ربما لا تشمل الأشعة السينية لكن ستكون بينها على الأقل الكاميرات والتسجيلات الصوتية. فيمكن لامرأة أن تلتقط صورة لإصابة أو أن تسجل سعالها وترسل المعلومات إلى طبيب أو أخصائي صحي يمكنها في ما بعد التواصل معه عن بعد بفعاليةٍ ومن دون تكاليف وعلى نحوٍ يراعي خصوصيتها. وإذا كانت الحلول الرقمية الشبيهة بهذه لا تمثل بديلاً مثالياً عن قطاع صحي جيد التشغيل، فإنها قادرة حتى ذلك الوقت على تقديم معلومات وطرق تفاعل جديدة ستخفف على الأقل من مشكلةٍ أكبر وأكثر عمقاً أرهقت أجيالاً عديدة.

العصبة العليا

ستعم فائدة الاتصالات على الجميع. فمن لا يستفيد منها اليوم سيستفيد منها قليلاً في الغد، ومن يستفيد منها كثيراً سيستفيد منها أكثر بعد. لإيضاح ذلك تخيل أنك أخصائي شاب يعيش في مدينة أمريكية بعد عقود من اليوم، عندها سيبدو أحد صباحاتك الاعتيادية شبيهاً بما يلي:

لن يشتملٍ روتين استيقاظك اليومي على ساعة منبه، على الأقل ليس بالمعنى التقليدي. بدلاً من ذلك سيوقظك عبير القهوة التي تم إعدادها طازجةً، إلى جانب الضوء الذي سيدخل غرفتك عندما يتم فتح الستائر آلياً، فضلاً عن تدليك الظهر اللطيف الذي يجريه لك سريرك عالي التقنية. وغالباً ما ستنهض من فراشك وأنت تشعر بقدر أكبر من الانتعاش بفضل حسّاس خاص يوضع داخل فراشك ليراقب إيقاعات نومك، حيث يحدد بدقة اللحظة المناسبة لإيقاظك من دون مقاطعة دورةٍ من دورات حركة العين السريعة.

ستكون شقتك عبارةً عن أوركسترا إلكترونية تقوم أنت بقيادتها. فمن خلال نقراتٍ بسيطةٍ على المعصم وبعض التعليمات المنطوقة يمكنك التحكم بدرجة الحرارة والرطوبة وبالموسيقى الخلفية والإضاءة، ويمكنك تصفح أخبار اليوم على شاشات شفافية (translucent) بينما تخرج بذلتك المنظفة للتو من خزانتك الآلية لأن تقويمك يشير إلى موعد اجتماع هام اليوم. ثم تتوجه إلى المطبخ لتناول الفطور فتتبعك شاشة الأخبار الشفافية، حيث سيكون مجسمٌ هولوغرافي مسلطاً أمامك تماماً، بينما تسير عبر الممر بالاعتماد على تقانة كشف الحركة. ستتناول بعد ذلك كوباً من القهوة، ومعجناتٍ طازجة تم تحضيرها حتى تنضج تماماً في فرنك مضبوط الرطوبة، فتقوم بعدها بتصفح البريد الإلكتروني الجديد على "صينية" هيلوغرافية مسلطةٍ أمامك. فيقترح نظام الحاسب المركزي لديك لائحة من الأعمال التي ستقوم بها روبوتاتك المنـزلية اليوم، فتوافق عليها جميعاً، ليتابع النظام اقتراحاته ويقترح عليك شراء صندوق قهوةٍ أكبر حجماً لاحَظَ وجود عرضٍ عليه على الإنترنت حالياً لأن مخزون القهوة لديك يتوقع أن ينفد يوم الأربعاء القادم. وكبديلٍ يعرض عليك بعض المراجعات الجديدة لخلطات قهوة استمتع بها أصدقاؤك مؤخراً.

بينما أنت تفكر في ذلك، تقوم بإخراج ملاحظاتك المتعلقة بعرض تقديمي ستجريه في وقت لاحق من اليوم لمجموعة مهمة من الزبائن من الخارج. وستكون جميع بياناتك المتعلقة بحياتك، الشخصية والمهنية على السواء، متوفرةً على جميع الأجهزة المختلفة لديك لأنها مخزنةٌ على السحابة؛ وهي نظام تخزين رقمي بعيد ذو سعة غير محدودة تقريباً. وسيكون لديك العديد من الأجهزة الرقمية المختلفة والقابلة للتبديل؛ أحدها بحجم الحاسب اللوحي وآخر بحجم ساعة الجيب، بينما تكون أجهزة أخرى مرنةً وقابلةً للحمل. وستكون جميعها خفيفة الوزن وسريعةً على نحوٍ لا يصدق، وتستخدم معالجاتٍ أقوى من أي شيءٍ نعرفه اليوم.

تتناول رشفةً أخرى من القهوة، وتمتلئ ثقة بأنك ستحوز على إعجاب زبائنك، فأنت تشعر مسبقاً بأنك تعرفهم مع أنك لم تلتق بهم شخصياً في السابق، فاجتماعاتكم كانت تُجرى من خلال واجهات واقع افتراضي؛ حيث كنت تتعامل مع تجسيدات هيلوغرافية تلتقط حركات زبائنك وكلامهم بدقةٍ بما يمكنك من فهمهم وفهم حاجاتهم بشكل جيد. وذلك ليس فقط لأن برمجيات الترجمة اللغوية المستقلة تعيد إنتاج كلام الطرفين في ترجمةٍ متقنة تكاد تكون لحظيةً، بل أيضاً لأن مثل هذه التفاعلات الافتراضية بالزمن الحقيقي، إضافةً إلى القدرة على تحرير الوثائق وتشاركها وغيرها من المشاريع؛ جميعها عوامل تجعل المسافة الفعلية بينكم تبدو مهملة.

في أثناء تجولك في المطبخ تصدم قدمك بحافة خزانة بقوة، فتتناول جهازك النقال وتفتح تطبيقاً تشخيصياً. داخل جهازك ثمة شريحة صغرية دقيقة تستخدم موجات ميليمترية منخفضة الإشعاع شبيهة بالأشعة السينية تمسح بها جسدك، فيكشف مسح سريع بأن قدمك مرضوضة وليست مكسورة، ثم ترفض الدعوة التي يوجهها لك جهازك لأخذ استشارة في عيادة طبيب قريب.

يبقى أمامك القليل من الوقت حتى يحين موعد مغادرتك إلى العمل الذي ستصل إليه بسيارة من غير سائق بالطبع، فسيارتك تعلم الوقت الذي يتوجب عليك فيه أن تكون في المكتب كل صباح بناء على جدول مواعيدك. وبعد تحليلها بيانات المواصلات تقوم سيارتك بالتواصل مع ساعة معصمك لتعطيك عداداً تنازلياً من ستين دقيقة يحدد لك موعد مغادرتك المنـزل. وستكون رحلتك على قدر عال من الإنتاجية، أو من الاسترخاء، وفقاً لما ترغب.

قبل أن تتوجه للمغادرة يذكرك جهازك بأن عليك أن تشتري هدية لابن أخيك بمناسبة ذكرى مولده، فتتفقد أفكار الهدايا التي يقترحها نظامك بناءً على بيانات مغفلة الهوية يتم تجميعها من صبيان في التاسعة من عمرهم يشاركون ابن أخيك اهتماماته. لكن، لا يعجبك أيّ من هذه الاقتراحات، فتتذكر قصةً أخبرك بها والداه جعلت كل من هو فوق الأربعين يضحك، حيث لم يستوعب ابن أخيك ما تعنيه الإشارة إلى العذر المعروف "لقد قضم الكلب واجبـي المدرسي"، فكيف يمكن لكلبٍ أن يأكل سواقة التخزين في السحابة؟ فهو لم يذهب إلى المدرسة قبل الكتب المدرسية الرقمية والمناهج التدريسية الشبكيّة، ونادراً ما كان يستخدم الورق لإنجاز واجباته، وكان معتاداً على استخدام وسائط التخزين في السحابة إلى

درجة أنه وجد فكرة نسيان واجبه المدرسي والخروج بعذرٍ كهذا بلا معنى. عندها تقوم بإجراء بحثٍ سريع عن كلب روبوتي وتشتري واحداً بنقرةٍ واحدة، وبعد إضافة بعض اللمسات الخاصة التي قد تعجبه، مثل هيكلٍ مقوى من التيتان يُتيح له الركوب عليه، تدوّن على البطاقة ملاحظة - "تحسباً" - ليصل الكلب إلى منـزله خلال فارق لا يتجاوز خمس دقائق عن موعد توصيل تحدده.

تفكر في تناول كوبٍ آخر من القهوة، لكن جهازاً تماسياً (التقانة التماسية تقانة تعتمد على اللمس والحس) مزروعاً في نعل حذائك يعطيك وخزةً لطيفة في إشارةٍ إلى أنك قد تتأخر على موعد اجتماعك الصباحي إذا تباطأت أكثر بعد. وربما تتلقف تفاحةً وأنت في طريقك للخروج لتأكلها وأنت جالس على المقعد الخلفي من سيارتك التي تقودك إلى مكتبك.

وإذا كنت أحد أفراد العصبة العليا من أصحاب الدخل في العالم (كما هو حال معظم سكان البلدان الغربية الغنية) فستتاح أمامك الكثير من هذه التقانات مباشرةً، إما كمالكٍ لها أو كصديقٍ لشخصٍ ما يملكها، ولعلك تلاحظ ضمن الروتينات الصباحية السابقة بعض الأشياء التي سبق لك أن تخيلتها أو عشتها. وسيكون هناك دائماً أولئك الأغنياء جداً بالطبع الذين ستكون التقانة متوفرةً لديهم على نحوٍ أعظم. ومن المرجح أنهم سيتحاشون السيارات برمتها لينتقلوا إلى عملهم في حواماتٍ آلية متوازنة الحركة على سبيل المثال.

ستبقى هناك تحديات نواجهها في العالم المادي، لكن توسع العالم الافتراضي، وما هو ممكن على الشبكة (إضافةً إلى انضمام خمسة مليارات عقل جديد) يعني أننا سنجد طرقاً جديدة للحصول على المعلومات ولتحريك الموارد لحل هذه المشكلات. ورغم أن هذه الحلول غير تامة، وفروقاً لا يستهان بها ستبقى موجودة بيننا، فإن توفر المزيد من فرص التفاعل واتباع سياسةٍ أفضل قد يساعد على التخفيف من هذه الفروق.

سيتجاوز أثر تطور الاتصالات المستوى الشخصي إلى حدٍّ بعيد، فالطرق التي سيتجاور بها العالمان المادي والافتراضي ويتصادمان ويكملان أحدهما الآخر ستؤثر على نحوٍ كبير في سلوك المواطنين والدول في العقود القادمة. وليست جميع الأخبار سارةً هنا، والفصول القادمة ستبحث في كيفية تعامل الجميع - من أفرادٍ وشركاتٍ ومنظماتٍ غير حكومية وحكومات وغيرها - مع هذا الواقع الجديد الذي يفرض التواجد في عالمين، وكيفية استغلال أفضل وأسوأ ما يمتلكه كلٌ من هذين العالمين في العصر الرقمي الجديد. وسيترتب على كل فرد اكتشاف معادلته الخاصّة؛ وكذلك الأمر بالنسبة إلى كل الحكومات وكل المنظمات. وأولئك الأقدر على التحرك ضمن هذا العالم متعدد الأبعاد سيجدون أنفسهم في المقدمة في المستقبل.

الفصل الثاني: مستقبل الهوية والمواطنة والتقارير الإخبارية

خلال العقد القادم، سيتجاوز عدد السكان الافتراضيين للأرض عدد سكانها الفعليين. حيث سيكون كل شخص ممَثَّلاً عملياً على الشبكة بعدة طرق، مما سينتج تجمعات حيوية وفعالة من المصالح المتداخلة التي تعكس العالم الحقيقي وتغنيه. وستنتج جميع هذه الارتباطات مقادير هائلة من البيانات (ثورة البيانات كما يسميها البعض) ستمنح المواطنين قوة لم يكن من الممكن تخيلها في السابق. لكن، بالرغم من هذه التطورات، سيبقى هناك محذور مركزي ووحيد: ستؤدي ثورة البيانات هذه إلى تجريد المواطنين من الكثير من السيطرة على معلوماتهم الشخصية في الفضاء الافتراضي؛ مما ستكون له آثار لا يستهان بها على العالم المادي. وإذا كان ذلك لا ينطبق على كل حالة أو على كل مستخدم، فسيكون له أثر بالغ على المستوى الماكروي يساهم من خلاله في تشكيل عالمنا. أما التحدي الذي يبقى أمامنا كأفراد فيتمثل في تحديد الخطوات التي نكون مستعدين لاتخاذها لاستعادة السيطرة على خصوصيتنا وأمننا.

تؤثر هوياتنا الشبكية اليوم على ذواتنا المادية، لكنها نادراً ما تطغى عليها. فما يقوله الناس أو يفعلونه على حساباتهم على الشبكات الاجتماعية قد يعود عليهم بالمديح أو النقد، لكن جل المعلومات الحساسة حقاً أو الشخصية يبقى محجوباً عن أنظار العامة. وعادة، تستهدف حملات التشويه الشخصيات العامة وليس المواطنين العاديين. أما في المستقبل، فستتحدد هوياتنا في الحياة اليومية أكثر فأكثر بطبيعة نشاطاتنا وعلاقاتنا الافتراضية. وسيكون لماضينا - الذي يكون على درجة عالية من التوثيق - أثر على الإمكانيات المتاحة أمامنا. وستزداد إلى حدٍّ بعيد قدرتنا على التأثير والتحكم بطريقة تلقي الآخرين لنا. وستزداد إمكانية وصول أحدهم إلى هوياتنا الشبكية في المستقبل ومشاركته لها وتلاعبه بأجزاء منها؛ وخصوصاً مع اعتمادنا على تخزين البيانات على السحابة. (إذا أردنا استخدام لغة غير تقنية، فإن حوسبة السحابة تعني البرمجيات المستودعة في الإنترنت والتي لا يحتاج المستخدم إلى إدارتها عن كثب. فتخزين المستندات أو المحتويات "على السحابة" يعني أن البيانات مخزنة على مخدمات بعيدة وليست على أجهزة محلية أو على حاسب الشخص نفسه؛ مما يتيح للعديد من الشبكات والمستخدمين إمكانية الوصول إليها. ومع حوسبة السحابة، تصبح النشاطات الشبكية أخف، وانتشارها أسرع، وتجهيزاتها أفضل في التعامل مع حمولات النقل). ستفرض هذه الثغرة، المُدركة والحقيقية في آن معاً، على شركات التقانة أن تبذل المزيد من الجهد لكسب ثقة مستخدميها. فإذا لم تتمكن من تجاوز آمالهم في ما يتعلق بكل من الخصوصية والأمن، فإن النتيجة ستكون إما تراجع منتجاتها أو التخلي عن هذه المنتجات كلياً. وصناعة التقانة تعمل منذ اليوم بكل جد لإيجاد طرق مبتكرة

للتخفيف من المخاطر من خلال التحقق المضاعف من الهوية مثلاً؛ حيث يطلب منك اثنان من البنود التالية حتى تتمكن من الوصول إلى بياناتك الشخصية: شيء ما تعرفه (أي كلمة المرور على سبيل المثال)، وشيء تملكه (أي الجهاز النقال)، وشيء تكونه (كما تبرهن بصمة الإصبع مثلاً). وثمة ما يدفعنا إلى الحماسة أيضاً عندما نعلم أن الكثير من أفضل المهندسين في العالم يعملون بجدٍ على مجموعة الحلول التالية. وأقل ما هناك هو أن يصبح التشفير القوي متوفراً في كل مكان تقريباً ليمثل حلاً أفضل وإن لم يكن مثالياً. ("التشفير" يعني خلط المعلومات حيث لا يمكن فك ترميزها واستخدامها سوى من قبل شخص يوفر متطلبات التحقق الصحيحة).

ربما تتغير أساسيات الهوية الشبكية. فقد تعتبر بعض الحكومات أنه من المجازفة بمكان السماح بوجود كل هذه الآلاف من المواطنين مغفلي الهوية الذين لا يمكن تتبع آثارهم أو التحقق منهم، مما يجعلهم بمثابة "أشخاص أخفياء". وبالتالي، سترغب هذه الحكومات بمعرفة الشخص المرتبط بكل حساب على الشبكة، وستطلب التحقق من الهويات - على مستوى الدولة - بما يسمح لها بممارسة قدر من السيطرة على العالم الافتراضي. من المستبعد أن تكون هويتك الشبكية في المستقبل مجرد صفحة على موقع الفيسبوك، حيث ستتكون من مجموعة من الحسابات من جميع الفعاليات الشبكية التي سيتم التحقق منها، بل وربما تنظيمها من قبل الحكومة. تخيل جميع حساباتك (على الفيسبوك وتويتر وسكايب وغوغل بلاس ونيتفليكس واشتراكك لدى نيويورك تايمز) مرتبطة . وضمن نتائج البحث، سيتم تصنيف المعلومات المرتبطة بحسابات شبكية تم التحقق منها ضمن رتبة أعلى من المحتويات التي لا تحمل مثل هذه الدمغة؛ مما سيدفع معظم المستخدمين إلى النقر بشكل طبيعي على المعلومات الأعلى (تحققاً). وعندها سيكون الثمن الحقيقي للبقاء من دون هوية هو عدم الظهور بين نتائج البحث. فحتى أكثر المحتويات جاذبية - إذا ارتبطت بحساب مغفل الهوية - لن يتم النظر إليها؛ ببساطة لأنه سيتم تصنيفها في مرتبة متدنية جداً.

سيكون للانتقال من هوية تتكون خارج الشبكة وتنعكس عليها إلى هوية يتم تشكيلها على الشبكة وتُمارس خارجها، آثار على المواطنين والدول والشركات في أثناء تجوالها في العالم الرقمي الجديد. وستحدد طريقة تعامل الناس والمؤسسات مع شؤون الخصوصية والأمن في هذه الحقبة الغنية بالمعلومات الحدودَ الجديدة للمواطنين في كل مكان. وما نسعى إليه هنا هو استكشاف ما يمكن أن تعنيه التواصلية الكاملة بالنسبة إلى المواطنين في المستقبل، وكيفية تمكنهم من الاستجابة لها، والتبعات التي ستكون لها في الدكتاتوريات والديمقراطيات على حدٍّ سواء.

ثورة البيانات

ستعود ثورة البيانات على مواطني المستقبل بمنافع غير مسبوقة. حيث سيتاح لهم فَهمٌ غير مسبوق لطريقة تفكير الناس وتصرفهم وتقيدهم بالمعايير أو خروجهم

عليها، سواء أتمّ ذلك في المنـزل أم في أي وسط اجتماعي في العالم. وستمهد القدرة الحديثة على استخراج معلومات دقيقة ومحققة من الشبكة، بسهولة وباللغات الأم وبكميات غير محدودة، لحقبة جديدة من التفكير النقدي في مجتمعات العالم التي كانت ذات يوم معزولة ثقافياً. أما في المجتمعات التي تعاني من ضعف البنى التحتية، فستمكن الاتصالات الناس من إقامة الأعمال ودفع الفواتير والتعامل مع حكوماتهم على مستوى جديد تماماً.

سيحمل المستقبل معه عهداً جديداً غير مسبوق، غنياً بالخيارات والبدائل. وبينما سيحاول بعض المواطنين إدارة هوياتهم بأقل قدرٍ ممكن من المشاركة الافتراضية، سيجد الآخرون أن الفرص التي تضمنها لهم هذه المشاركة تستحق المجازفة بكشف هذا المقدار من الخصوصية. وستصل مشاركة المواطنين إلى مستوى لم تصله من قبل مع تمكن أي شخص يملك جهازاً نقالاً واتصال إنترنت من المشاركة في عملية الترويج للمحاسبة والشفافية. فسيتمكن صاحب متجرٍ في أديس أبابا مع مراهقٍ صغير من سان سلفادور من نشر معلوماتٍ حول الرشى والفساد، والإبلاغ عن تجاوزاتٍ في الانتخابات، ومحاسبة الحكومة بشكلٍ عام. ستساعد كاميرات الفيديو المركبة على سيارات الشرطة في المحافظة على نـزاهة الشرطة إذا لم تكف الكاميرات الموجودة في هواتف المواطنين وحدها. بل ستمنح التقانة الناس القدرة على أن يكونوا شرطة على الشرطة بطرقٍ مبتكرة لم تكن يوماً ممكنة؛ كنظم المراقبة بالزمن الحقيقي التي تسمح للمواطنين بتقييم كل ضابط شرطة في منطقتهم علناً. وستصبح جميع أنظمة التجارة والتعليم والرعاية الصحية والعدل أكثر فعاليةً وشفافيةً وشمولاً مع دخول المؤسسات الكبرى العصر الرقمي.

سيكون على من يحاولون تخليد أساطير دينية أو ثقافية أو إثنية أو غيرها أن يكافحوا للإبقاء على حكاياتهم طافية في لجة بحر من المستمعين المزودين بالمعلومات الحديثة. فمع توفر المزيد من البيانات سيكون كل شخص قادراً على بناء إطار مرجعي أفضل. وقد يجد طبيب مشعوذ من مالاوي أن مجتمعه قد أصبح يعاديه فجأة إذا وصل الناس إلى معلومات على الشبكة تتناقض مع سلطته واقتنعوا بها. وقد يواجه الشباب في بلد ما كبار قبيلتهم بمسألة الزواج المبكر للفتيات - الذي يتم وفقاً للتقاليد - إذا ارتأوا أن معظم الأصوات على الشبكة مجمعة على مناهضته، وأنه بالتالي يسيء إلى صورتهم كأفراد. أو قد يجد أتباع رجل هندي طريقة يقاطعون بها بين مزاعمه على الإنترنت ليتخلوا عنه إذا تبيّن لهم أنه كان يضللهم.

بينما تشكل ظاهرة الانحياز التأكيدي (أي أن يصب الناس اهتمامهم على مصادر المعلومات التي تؤكد نظرتهم إلى العالم عن وعي أو من دونه) مصدر قلق للكثيرين مع توافر مصادر المعلومات على الإنترنت، توصلت دراسة حديثة لجامعة ولاية أهايو إلى أن هذه الظاهرة أضعف مما كان يعتقد؛ على الأقل ضمن المشهد السياسي الأمريكي. فالانحياز التأكيدي يتعلق في الواقع بردّ فعلنا إزاء معلومات نتلقاها سلبياً بقدر ما يتعلق بميولنا لاختيار مصادر المعلومات على نحوٍ فاعل. لذا، يحق لنا أن نتفاءل حيال التغييرات الاجتماعية القادمة؛ مع وصول ملايين البشر إلى الشبكة.

ستجد الحكومات بدورها صعوبة في المناورة مع ازدياد تواصل مواطنيها، فالتصرفات التقييدية والقمعية مثل إخفاء الوثائق أو الخطف أو تدمير النصب التذكارية ستفقد الكثير من فعاليتها الوظيفية والرمزية في العصر الرقمي الجديد. حيث ستكون الوثائق قابلةً للاستعادة بعد أن يكون قد تم تخزينها على السحابة. وسيكون بإمكان جمعية فعالة ومعولمة على الإنترنت حين تعبئ قدراتها ضد الظلم أن تمارس من الضغط ما يدفع الحكومات إلى التفكير جيداً قبل القبض على أي شخصٍ أو سجنه تعسفياً. وسيبقى بوسع حكومة مثل حكومة طالبان أن تدمر أوابد تاريخيةً مثل تماثيل بوذا في ولاية باميان، لكن هذه الصروح ستكون في المستقبل قد خضعت للمسح بواسطة تقانة متقدمة تحفظ كل زاوية وكل شق فيها في ذاكرة افتراضية تسمح بإعادة بنائها لاحقاً بواسطة طابعات ثلاثية الأبعاد، أو حتى تسليطها على شكل هولوغرام. ربما يقوم مركز الإرث العالمي التابع لليونسكو بإدراج هذه الإجراءات ضمن جهود الترميم التي يمارسها، أو إعادة بنائه باستخدام الطباعة ثلاثية الأبعاد في موقعه الأصلي في دورا إيروبوس. وما هو واقعٌ قائمٌ في معظم البلدان النامية، أي وجود مجتمع مدني ناشط وعازم على محاسبة حكومته والتحقيق معها، سينتشر في كل مكانٍ تقريباً بفضل انتشار أجهزة رخيصة وفعالة بشكل أساسي. على مستوى أدنى من ذلك، سيكون بمقدور المواطنين في كل مكان أن يقارنوا أنفسهم وطريقة حياتهم ببقية الناس. وفي هذا السياق، ستبدو الممارسات التي تبدو على نحو متفق عليه بربرية أو متخلفة أشدّ بربرية وتخلفاً بعد.

ستصبح الهوية هي السلعة الأغلى ثمناً بالنسبة إلى المواطنين في المستقبل، وستتواجد بشكل رئيس على الشبكة. وستبدأ التجربة الشبكية منذ الولادة، وربما قبل ذلك، فستبدو مراحل معينة من حياة الأفراد وكأنها جامدة زمنياً، وسيكون الكشف عنها ممكناً بسهولة ليراها الجميع. وسيترتب على الشركات - استجابة لذلك - أن تنتج أدوات جديدة للتحكم بالمعلومات مثل اللوائح التي تمكن الناس من إدارة من يرى بياناتهم. أما تقانات الاتصالات التي نستخدمها اليوم فهي اجتياحية في تصميمها، حيث تجمع صورنا وتعليقاتنا وأصدقاءنا في قواعد بيانات عملاقة يمكن البحث فيها، وتمثل - في غياب التشريعات الخارجية - فريسةً سهلة لأصحاب العمل وكوادر القبولات في الجامعات ولنمائم المدينة. فقل لي ما تغرد أقل لك من أنت.

خارجة عن الزمن بدلاً من جامدة زمنياً

في الحالة المثالية، سيتوفر لدى الناس الوعي الذاتي الكافي لإدارة هوياتهم الشبكية والحياة الافتراضية التي يعيشونها عن كثب، حيث يراقبونها ويشكلونها منذ عمرٍ مبكر من دون أن يحدّوا من الإمكانيات المتاحة أمامهم في الحياة. لكن هذا مستحيل بالطبع، فالأطفال والمراهقون لديهم دوافع للمشاركة تغلب دائماً على المجازفات الغامضة والبعيدة التي يفرضها الكشف عن الذات؛ حتى بوجود أمثلةٍ بارزة تبيّن للجميع عواقب ذلك. وعندما يصل المرء إلى العقد الرابع من عمره،

سيكون قد كدّس وخزّن سرداً شاملاً على الشبكة؛ يحتوي جميع الحقائق والروايات المتخيلة، وكل هفوة وكل نصر حققه على امتداد حياته كلها. وحتى الإشاعات ستعيش إلى الأبد.

وقد نشهد في المجتمعات المغرقة في المحافظة، والتي يولى فيها للعار الاجتماعي وزنٌ كبير، نوعاً من أي تكريس الجهود لتدمير الهوية الشبكية لشخص ما سواء أكان ذلك وقائياً (عبر الكشف عن ذنوب تمت ملاحظتها أو زراعة معلومات زائفة) أم ردّ فعل (عبر ربط هوية الشخص الشبكية بمحتوى يروي تفاصيل جريمة ما، سواء أكانت حقيقية أم متخيلة). وإذا كانت السمعة الشبكية المدمرة لا تقود إلى عنفٍ جسدي من قبل مرتكبها، فإن امرأة شابة تواجه مثل هذه الاتهامات ستجد نفسها موصومةً بحرفٍ قرمزيٍ رقمي لن تتخلص منه في حياتها نتيجةً لحظ عاثر لا يمكن منعه منح بياناتها الخلود. وقد يدفع هذا العار العلني أحد أفراد عائلتها إلى قتلها.

فماذا عن دور الوالدين؟ يعلم كل من لديه أطفال أن دور الوالدين ليس سهلاً. ومع أن العالم الافتراضي قد يصعب هذا الدور، إلاّ أنه ليس تعجيزياً. إذ ستكون للوالدين في المستقبل المسؤوليات نفسها، لكن عليهما أن يُبدوَا مشاركةً أكبر إذا أرادا ضمان عدم وقوع أبنائهما في أخطاء على الشبكة قد تؤثر على مستقبلهم المادي. وبما أن الأطفال يعيشون حياة أسرع بكثير على الشبكة مما يسمح به نضوجهم الجسدي، فسيدرك معظم الأهالي أن أثمن طريقة لمساعدة أطفالهم هي في أن يكون الحديث عن الخصوصية والأمن سابقاً للحديث عن الجنس. وسيكتسب التكتيك القديم الذي يتمثل بأن يفاتح الأهل أطفالهم قيمة هائلة.

ستتكيف النظم المدرسية مع ذلك؛ حيث تلعب دوراً هاماً أيضاً. وستدافع جمعيات الأهالي والمدرسين عن فكرة تقديم دروس في الخصوصية والأمن إلى جانب صفوف الثقافة الجنسية في المدارس. وسيتعلم الطلاب في مثل هذه الصفوف كيفية التحكم بإعدادات الخصوصية والأمان لديهم، وسيتدربون على تشرّب توصيات العالم الافتراضي ومحاذيره، وسيخيفهم المدرسون بقصص من الحياة الواقعية تبين ما يحدث إذا لم يسيطروا على خصوصيتهم وأمنهم في مرحلةٍ عمرية مبكرة.

لا شك في أن بعض الأهالي سيحاولون المقامرة بالنظام أيضاً عبر حلولٍ خوارزمية قد تؤثر أو لا، ولنا في عملية تسمية الطفل مثال على ذلك. فمع ازدياد القيمة الوظيفية للهوية الشبكية، سيلعب إشراف الوالدين دوراً حاسماً في المراحل المبكرة من الحياة؛ بدءًا من اسم الطفل. ومن المعروف أن ستيفن د. ليفيت وستيفان ج. دوبنر مؤلفي الكتاب الاقتصادي الشعبـي **غرائب الاقتصاد** قد شرحا كيف أن الأسماء الشائعة إثنياً (وتحديداً الأسماء الشائعة في الأوساط الأفروأمريكية) قد تكون مؤشراً على فرص نجاح الأطفال في الحياة. وإذا أراد الوالدان أن يسبقا الوقت، فعليهما أن يفكرا في أثر تصنيف نتائج البحث الشبكية على مستقبل طفلهما. فالوالد ذو التفكير الاستراتيجي حقاً سيتجاوز مسألة حجز حسابات الشبكات الاجتماعية وشراء أسماء النطاق (مثل جون ديفيد سميث.كوم)

وسيختار بدلاً عن ذلك أسماء تؤثر على مدى سهولة أو صعوبة العثور على أطفاله عبر الشبكة. وسيعمد بعض الأهالي إلى اختيار أسماء نادرة أو أسماء تقليدية مهجَّأة بطريقة غير معتادة تجعل أبناءهم متميزين ضمن نتائج البحث، مما يسهل العثور عليهم والترويج لهم عبر الشبكة، ويخفف عنهم المنافسة المباشرة. بينما سيسلك آخرون الطريق المعاكس بأن يختاروا أسماء شائعةً وبسيطة تسمح لأبنائهم بالعيش في العالم الشبكي مع درجةٍ من الحماية من فهارس الإنترنت، فيكون الطفل مجرد آخرٍ بين آلاف المدخلات المشابهة.

سنشهد أيضاً تكاثراً للأعمال التجارية التي تهتم بشؤون الخصوصية والسمعة، وهي صناعةٌ موجودةٌ منذ الآن عبر شركاتٍ مثل ريبوتيشن.كوم التي تستخدم تشكيلة من التكتيكات الفاعلة والمتفاعلة لإزالة المحتويات غير المرغوب فيها من الإنترنت أو لتخفيفها*. وقد أفيد خلال الانهيار الاقتصادي لعام 2008 بأن العديد من مصرفيي وول ستريت قد كلفوا شركات سمعة شبكية بالتخفيف من حضورهم على الشبكة متكبدين دفع مبالغ كبيرة تصل إلى عشرة آلاف دولار في الشهر مقابل هذه الخدمة. ستتنوع هذه الصناعة في المستقبل مع انفجار الطلب عليها، حيث يصبح مديرو الهوية منتشرين كما هو حال سماسرة البورصة والمخططين الماليين اليوم. وستصبح الإدارة الفاعلة للحضور الشبكي للشخص (عبر تلقي تقارير فصلية من مدير هويتك مثلاً يتتبع فيها التغير في شكل هويتك الشبكية) هي العادة الجديدة للشخصيات البارزة أو لأولئك الذين يطمحون إلى التحول إلى شخصياتٍ بارزة.

سيظهر حقل جديد للتأمين أيضاً. حيث ستعرض الشركات تأميناً على هويتك الشبكية ضد السرقة والاختراق والاتهامات الكاذبة وإساءة الاستخدام والاستيلاء. فقد يستخرج الوالدان مثلاً بوليصة تأمين ضد أضرار السمعة التي قد تنجم عما يقوم به أبناؤهما على الشبكة. وقد تستخرج مدرسة بوليصة تأمين تحميها ضد اختراق تلميذ فيها حسابها على الفيسبوك، وتغييره تفاصيل حسابها الشبكي بطريقة تحرجها أو تشوه سمعتها. واليوم ثمة شركات حماية ضد سرقة الهوية، لكننا في المستقبل سنشهد شركات تأمين تعرض حماية زبائنها ضد إساءاتٍ دقيقةٍ جداً. وقد تجتذب بوليصة تأمين كهذه الكثير من الناس، سواء أكانوا في حاجة إليها فعلاً أم كانوا بشكلٍ عام متشكّكين وحسب.

ستصبح الهوية الشبكية عملة قوية إلى درجة أننا سنشهد ظهور سوق سوداء جديدة يمكن فيها للناس شراء هويات حقيقية أو مخترعة. وستجتذب مثل هذه الشبكة المواطنين والمجرمين على حدٍّ سواء؛ بما أن الهوية المزيفة التي يمكنها التغطية على مهرب مخدرات معروف يمكنها أيضاً أن تحمي معارضاً سياسياً. وسيتم تصنيع هذه الهوية أو سرقتها، وستكون مرفقة بما يتممها من مدخلات تعود إلى تواريخ سابقة وسجلات أنشطة مرفقة بعناوين إنترنت وبأصدقاء وعمليات شراء مزيفة وطرق أخرى تجعلها تبدو مقنعة. فإذا احتاجت عائلة شخص مكسيكي لديه معلوماتٌ تدين شخصاً ما إلى الهرب من العنف في مدينة سيودات خواريز وكانت تخشى من عقوبة الائتلاف السياسي، فإن مجموعة من الهويات الشبكية

المزيفة ستساعدها بالتأكيد على التغطية على المسارات التي تسلكها وتؤمن لها سجلاً نظيفاً.

بالطبع، إن هذا النوع من طرق الهرب يعتبر محاولةً محفوفةً بالمخاطر في العصر الرقمي. فالحياة الجديدة تتطلب الانفصال التام عن الروابط السابقة؛ لأن مجرد إشارة صغيرة (مثل عملية بحث عن قريب) قد تشي بالشخص. علاوةً على ذلك، سيتوجب على أي شخص ينتحل هوية مزيفة أن يتجنب جميع الأماكن التي توجد فيها تقانة التعرف على الوجوه خشية أن يتم مسح وجهه والتعرف على حساب قديم له. ولن تكون هناك أزقة مظلمة في هذه السوق غير الشرعية أيضاً، حيث يمكن شراء جميع الهويات عبر اتصالاتٍ مشفّرة تتم بين أطراف مغفلي الهوية، ويتم التسديد لهم بواسطة عملة افتراضية يصعب تعقبها. سيواجه الوسطاء والمشترون في هذه المقايضة مخاطر شبيهة بتلك التي يواجهها العاملون في الأسواق السوداء اليوم كالعملاء المتخفين والتعاملات غير النـزيهة (التي ربما تصبح الأكثر احتمالاً بسبب الطبيعة مغفلة الهوية للتعاملات في هذا العالم الافتراضي).

سيهلل البعض لانتهاء إمكانية التحكم نتيجة الاتصالات والبيئات الغنية بالبيانات. وهؤلاء هم من يعتقدون أن "المعلومات تريد الحرية"*، وأن المزيد من الشفافية في جميع النواحي سينتج عالماً أكثر عدلاً وأماناً وحرية. وقد كان جوليان أسانج، أحد مؤسسي موقع ويكيليكس، أبرز سفراء هذه القضية في العالم لفترة من الزمن. لكن أنصار ويكيليكس والقيم التي يدافع عنها ينتمون إلى مختلف المشارب؛ من مؤيدي الحريات في الجناح اليميني، إلى الليبراليين في أقصى اليسار والمتحمسين للتقانة السياسية. فهؤلاء، وإن لم يُجمِعوا على التكتيكات دائماً، يعتبرون ديمومة البيانات صمام أمان للمجتمع. وبالرغم من بعض التبعات السلبية المعروفة لهذه الحركة (كتهديدها أمن الفرد، وإمكانية تدميرها السمعة، وتسببها بالفوضى الدبلوماسية) يعتقد بعض الناشطين المؤيدين لحرية المعلومات أن غياب زر الحذف يعزز في النهاية مسيرة الإنسانية نحو العدالة والإنتاجية وحق تقرير المصير. إلا أننا نعتقد أن هذا النموذج خطير، خصوصاً على اعتبار أنه سيكون هناك دائماً شخص ما سيئ الحكم يصدر معلومات تؤدي إلى مقتل بعض الناس. وهذا هو ما يدفع الحكومات إلى تبني نظم وتشريعات قيمة يفترض بها، وإن لم تكن تامةً، أن تحدد الشخص المخول باتخاذ القرار حول تحديد ما هو سري وما هو غير سري.

وقد تحدثنا مع أسانج في حزيران من عام 2011؛ بينما كان رهن الإقامة الجبرية في المملكة المتحدة. وبعيداً عن موقفنا المذكور آنفاً، لا بد لنا من أن نأخذ في الحسبان مستقبلاً ما حاول ناشطو حرية المعلومات القيام به. وبالتالي، إن أسانج نقطة انطلاقٍ مفيدة. ونحن لن نكرر هنا المناقشات الجارية اليوم (التي ألفت فيها الكتب والمقالات مسبقاً)، والتي تركز بشكلٍ أساسي على رد الفعل الغربـي على ويكيليكس، وعلى محتويات الرسائل التي تم تسريبها، وعلى مدى التخريب الذي تؤدي إليه هذه التسريبات، والعقوبات التي يجب أن تنتظر أولئك المتورطين في مثل هذه الفعاليات، بل سنركز بدلاً عن ذلك على المستقبل، وعلى المرحلة التالية

لحركات حرية المعلومات (بدءاً بنموذج أسانج من دون أن نحصر أنفسنا به)، وما قد تحاول إنجازه أو تدميره. فخلال المقابلة، دفع أسانج بحجتين أساسيتين في هذا الخصوص تتعلق إحداهما بالأخرى. فهو يرى أولاً أن حضارتنا الإنسانية قائمةٌ على سجلنا الفكري الكامل، لذا يجب أن يكون هذا السجل واسعاً قدر المستطاع لكي يشكل عصرنا ويصل إلى أجيال المستقبل. ثانياً، لأن العديد من الفاعلين سيسعون دائماً إلى تدمير أجزاءٍ من هذا التاريخ المشترك انطلاقاً من مصالح ذاتية أو تغطيتها، لا بد لكل من يسعى إلى الحقيقة ويقدر ثمنها أن يحاول دخول هذا السجل قدر ما هو ممكن، ومنع الحذف منه، ثم جعل هذا السجل متاحاً للناس وقابلاً للبحث في كل مكان قدر الإمكان.

إن ما لدى أسانج ليس حرباً على السرية بحدّ ذاتها: "فثمة أسباب لا حصر لها تدفع المنظمات غير السلطوية إلى اللجوء إلى السرية"، كما أخبرنا، "وإنني أرى أن ذلك عمل مشروع، فهي تحتاج إليها بغياب السلطة"، بل إنه نضال ضد السرية التي تغطي على أفعالٍ لا تصبّ في مصلحة العامة. سألنا أسانج بوضوح: "لماذا تلجأ المنظمات السلطوية إلى السرية؟". وكان جوابه هو أن خططها ستكون عرضة للاعتراض عليها إذا أعلنت، بينما من شأن السرية أن توصلها إلى مرحلة تحقيق أهدافها، وهي النقطة التي يكون الأوان فيها قد فات على تغيير مسار الأحداث على نحوٍ فعال. أما المنظمات التي لا تثير خططها اعتراض العامة فلا مشكلة لديها مع السرية؛ لذا إنها لا تحتاج إليها، يضيف أسانج. ومع احتدام الصراع بين هذين النوعين من المنظمات ستطفو منها في النهاية تلك التي تتمتع بدعمٍ شعبـي أصيل، كما يقول أسانج، وعندها يكون الكشف عن المعلومات "إيجابياً بالنسبة إلى المنظمات التي تلتزم بنشاطاتٍ يدعمها العامة، وسلبيةً بالنسبة إلى المنظمات المنخرطة في نشاطاتٍ لا يدعمها العامة".

أما في ما يتعلق بالحجة القائلة إن مثل هذه المنظمات السرية يمكنها ببساطة أن تسحب عملياتها وتخرج بها من الشبكة تجنباً لفضحها، فإن أسانج واثق من قدرة حركته على منع ذلك. "هذا غير ممكن - يقول أسانج - فالمنظمات الجادة ستترك دائماً أثراً ورقياً". ويتابع موضحاً: "فالظلم المنظم يحتاج بالتعريف إلى استخدام الكثير من الناس". ولن يخول جميع المشاركين بالوصول إلى المخططات، لكن لا بد لكل منهم أن يعرف شيئاً ما لكي يتمكن من إنجاز مهامه. "أما عندما تخرج معلوماتك من الورق، أي عندما تخرجها من مسارها الورقي، الإلكتروني أو المادي، فإن المؤسسات تتحلل. وهذا هو السبب في وجود آثار ورقية دقيقة لدى جميع المنظمات تحتوي على تعليمات من القيادة". الآثار الورقية تضمن تنفيذ التعليمات على النحو المطلوب. لذا، يقول أسانج: "إذا قاموا بالتقسيم الداخلي حيث لا يمكن للمعلومات أن تتعرض إلى التسرب، فستكون تكلفة ذلك على الفعالية التنظيمية باهظة". والمنظمات غير الفعالة منظمات أقل قوة.

أما الانفتاح، من جهة أخرى، فإنه يفرض تحديات على حركة الباحثين عن الحقيقة هذه كما يرى أسانج. "فعندما تصبح الأشياء أكثر انفتاحاً تصبح أكثر تعقيداً أيضاً؛ لأن الناس يبدأون بإخفاء ما يفعلونه، أي سلوكهم السيئ، عبر التعقيد"، كما

يقول. ثم أشار إلى ازدواجية الخطاب البيروقراطي وإلى القطاع المالي القائم وراء البحار كمثالين واضحين، حيث يقول إن هذين النظامين منفتحان من الناحية التقنية، لكنهما في الحقيقة منيعان على الاختراق، ومن الصعب مهاجمتهما، لكن الأصعب هو استخدامهما بفعالية. ويكون الإخفاء على هذا المستوى - الذي يكون التعقيد فيه قانونياً لكنه يغطي على شيء ما مع ذلك - أصعب بكثير من التهرب من الرقابة المباشرة.

لسوء الحظ، إن أشخاصاً مثل أسانج يتمتعون بالموقع المناسب الذي سيسمح لهم بالاستفادة من بعض التغييرات التي سيشهدها العقد القادم؛ وكذلك الأمر بالنسبة إلى المنظمات مثل ويكيليكس. لكن أنصارهم يواجهون أسئلة صعبة حول طرائق التسريبات على الإنترنت ومضاعفاتها، وخصوصاً إذا نظرنا إلى ما هو أبعد من حالة ويكيليكس عينها في المستقبل. وأحد أصعب هذه الأسئلة هو سلطة التقدير، فمن الذي سيقرر في النهاية المعلومات المناسب إطلاقها، وما يجب إعادة صياغته، ولو مؤقتاً؟ ولماذا يكون جوليان أسانج بالذات هو الذي يحدد المعلومات التي تهم الرأي العام؟ وماذا لو كان ذلك الشخص الذي يتخذ مثل هذه القرارات مستعداً للقبول بضرر محقق سيلحق بالأبرياء من جراء عمليات التسريب التي يقوم بها؟ سيتفق معظم الناس على أن مستوى معيّناً من الرقابة لا بد منه في أية منصة تسريب تسعى إلى القيام بدور إيجابـي في المجتمع. لكن، ما من شيء يضمن أن تكون الرقابة موجودة فعلاً (ويتأكد لنا ذلك إذا ألقينا نظرة على مدى الطيش الذي ينشر به المخترقون* المعلومات الشخصية للآخرين على الإنترنت كما هي).

إذا كانت هناك هيئة مركزية تيسر عملية إطلاق المعلومات، فلا بد من وجود شخصٍ ما، أو مجموعة من الأشخاص - ممن لديهم أفكار وميول - المسؤولين عن اتخاذ هذه القرارات. وطالما أن البشر وليس الحواسب هم الذين يسيرون الأشياء في عالمنا، فسيترتب علينا دائماً مواجهة هذه الأسئلة المتعلقة بالحكم؛ مهما كان مدى شفافية هذه المنصات وسلامتها من الناحية التقنية.

إذا نظرنا إلى المستقبل، فإن بعض الناس قد يفترضون أن نمو الاتصالات حول العالم سيحفز انتشار منصات شبيهة بويكيليكس، وسيرجعون ذلك إلى تزايد عدد مستخدمي الإنترنت، وتوفر المزيد من المعلومات الخصوصية والسرية على الإنترنت؛ مما سيؤدي إلى ظهور عشرات المنصات الأصغر حجماً والمتخصصة في نشر الأسرار تلبية للزيادة بالعرض والطلب. إنها فكرة مقنعة ومخيفة، لكنها غير صحيحة، فثمة حواجز طبيعية تقف عائقاً أمام النمو في مجال مواقع الوب المتخصصة في فضح الأسرار، ومن بينها عوامل خارجية تحدّ من عدد المنصات التي يمكنها أن تتعايش بنجاح. وبغض النظر عن رأي المرء بويكيليكس، لا بد من التفكير في جميع الأشياء التي احتاج إليها لكي يصبح علامةً عالميةً معروفة: أكثر من تسريب واسع النطاق يكون ذا أهمية جيو - سياسية لجذب الاهتمام على المستوى الدولي، سجل متابعة للتسريبات يبيّن الالتزام بالقضية وينتج الثقة العامة ويمنح الحوافز للمسربين المحتملين الآخرين عبر إقناعهم بقدرة ويكيليكس على

حمايتهم، ورئيس صوري كاريزماتي قادر على تجسيد المنظمة وعلى لعب دور مانع الصواعق - كما سمى أسانج نفسه - ودفق مستمر من التسريبات الجديدة (غالباً ما تكون بالجملة) لكي تحافظ المنصة على اهتمام الجمهور بها، إضافةً إلى منصةٍ رقمية متطورةٍ تقنياً تكون على الأقل موزعةً توزيعاً كبيراً؛ حيث يستخدمها المسربون والعاملون في المنظمة إضافةً إلى الجمهور لمعالجة المواد المسربة (بينما يبقى هؤلاء جميعاً مجهولين في ما بينهم)، لكي تتمكن من تجنب إغلاقها من قبل السلطات في عديدٍ من البلدان. فبناء مثل هذا النظام المعقد والمرن في غاية الصعوبة، سواء أكان ذلك من الناحية التقنية أم بسبب اعتماد مختلف مكوناته في قيمتها على قدرات المكونات الأخرى. فما فائدة منصة متطورة من دون مسرّبين يملكون حوافز كافية؟ وما فائدة مجموعةٍ من الأسرار القيمة من دون نظامٍ يسمح بمعالجتها ونشرها، كل على حدة؟ لقد استغرق الوصول إلى هذا التوازن الذي حققه ويكيليكس - بين المصلحة العامة والتسريب الخصوصي والحمايات التقنية - سنوات طويلة، لذا يصعب تخيل ظهور فروع له أو منافسين أو حديثي نعمة في المستقبل يقومون ببناء منصةٍ شبيهة تحقق شهرةً أسرع. خصوصاً اليوم؛ بعد أن أصبحت السلطات في أنحاء العالم مدركة للتهديد الذي تمثله مثل هذه المنظمات.

علاوةً على ذلك، حتى إذا نجحت منظمات جديدة في بناء مثل هذه المنصات، فإنه من غير الوارد أبداً أن يتمكن العالم من دعم أكثر من مجموعة من هذه المنصات في أي وقت معطى. وثمة عدة أسبابٍ لذلك؛ أولها أنه حتى أدسم التسريبات تتطلب متابعة وسائل الإعلام لها لكي تحدث أثراً، فإذا أصبح مشهد مواقع إفشاء الأسرار أكثر تبعثراً، فستجد منافذ الإعلام صعوبةً في تتبع هذه المواقع وتسريباتها، وفي التحقق من مدى صدقيتها كمصدر. ثانياً، سيتحلق المسربون عفوياً حول المنظمات التي يعتقدون أنها تحدث الأثر الأعظم لتسريباتهم؛ بينما توفر لهم أكبر قدرٍ من الحماية. وقد تتنافس هذه المواقع على المسربين مقدمةً وعوداً بأشكال أفضل بعد من الانتشار وإغفال الهوية. لكن، يبقى من المنطقي أن المسربين المحتملين سيبحثون عن أمثلة ناجحة، وسيقتدون بمن سبقوهم من المسربين. فأي مصدرٍ سيجازف بفرصته - بل وبحياته - مع مجموعةٍ لم يتم تجريبها من قبل؟ أما المنظمات التي لا تنجح في اجتذاب تسريباتٍ عالية المستوى بشكلٍ مستمر، فإنها ستفقد الاهتمام والتمويل وستدخل عملية ضمور بطيئة لكنها أكيدة. وقد اعتبر أسانج هذه الدينامية، من وجهة نظر منظمته، دينامية إيجابية تفرض شروطاً على ويكيليكس لكنها بالقدر نفسه تحافظ على استمراره. فهو يقول: "المصادر تعبر عن رأيها عبر الأماكن التي تختار الانتقال إليها، ونحن مقيدون بقوى السوق". ربما تكون المناطقية هي ما سيحدد مستقبل مواقع التسريبات أكثر من أي شيء آخر. فمعظم الحكومات والشركات في الغرب تعي المخاطر التي تنطوي عليها هشاشة الأمن الرقمي، وحتى إذا لم تكن نظمها منيعةً تماماً على الاختراق، فإن موارد لا يستهان بها يجري استثمارها في كلٍّ من القطاعين العام والخاص لحماية السجلات وبيانات المستخدمين والبنية التحتية. لكن الأمر مختلف في معظم البلدان النامية، ويمكننا توقع أن تعيش بعض هذه الشعوب نسختها الخاصة من

ظاهرة الويكيليكس عندما تدخل عالم الإنترنت في العقد القادم: أي وجود مصادر قادرة على الوصول إلى سجلات مرقمنة حديثاً، وتملك الدافع لتسريب مواد حساسّة بهدف إحداث أثر سياسي، وربما تنحصر العواصف الناتجة عن ذلك ببلدٍ أو منطقةٍ معينة، لكنها ستبقى مع ذلك ذات أثرٍ عميق وأهميةٍ كبيرة في البيئات التي تلامسها، بل إنها قد تثير ثورةً أو تمرداً في العالم المادي. وعلينا أيضاً أن نتوقع انتشار تكتيكات مشابهة من قبل السلطات الحكومية لمكافحة مثل هذه المواقع (حتى إذا كانت هذه المنظمات ومخدماتها موجودةً في أمكنةٍ أخرى): الفلترة، والهجومات المباشرة، والمحاصرة المالية، والملاحقة القانونية.

أخيراً، إن التقانة المستخدمة في هذه المنصات ستصبح متطورةً إلى حدٍّ يجعلها غير قابلة للحجب عملياً. فعندما فقد موقع ويكيليكس عنوانه الرئيس المنتهي بأورغ بسبب سلسلة من هجومات حجب الخدمة، إضافة إلى سحب مزود خدمة الإنترنت الخاص به (الذي كان يستضيف الموقع) عام 2010، سارع أنصاره مباشرةً إلى إعداد أكثر من ألف موقعٍ "مرآة" (أي نسخ من الموقع الأصلي تستضاف في مواقع بعيدة) تحمل عناوين تنتهي بـ fe (في فنلندا) وce (في كندا) أو info (في هجوم حجب الخدمة يهاجم عددٌ كبير من الحواسب المخترقة هدفاً واحداً، مغرقاً النظام بطلبات المعلومات مما يتسبب بإغلاقه وحجب خدمته عن المستخدمين الحقيقيين). ولأن موقع ويكيليكس كان مصمماً كنظامٍ موزع (بمعنى أن عملياته كانت متوزعةً على كثيرٍ من الحواسب المختلفة بدلاً من أن تكون متركزةً في محور مركزي)، فإن إغلاق المنصة كان أصعب بكثير مما كان يبدو لمعظم الأشخاص العاديين. ولا شك في أن مواقع التسريبات في المستقبل ستتجاوز تقنية المواقع المرآة (أي إجراء نسخ من الموقع الأصلي) مستخدمة طرائق جديدة لتكرار عملياتها وجعلها مبهمةً لكي تحمي نفسها من السلطات. وسيكون من بين الطرق الممكنة لتحقيق ذلك إنتاج نظام تخزين تنسخ فيه مجتزآت من الملفات وتوزع بطريقةٍ تسمح بإعادة تجميع الملف الأصلي إذا تعرض أحد أدلة الملفات للإغلاق. وستطوِّر هذه المنصات طرقاً جديدة تضمن إغفال هوية المسربين المحتملين عند التسليم. فموقع ويكيليس يحدّث طريقة التسليم لديه باستمرار، ويحذر مستخدميه من قنوات التشفير السابقة (مثل أس.أس.أل، أو طبقة المقبس الآمن، وخدمة البوابة المخفية التي تستخدم شبكة تور عالية التشفير)، حيث سبق أن وجدوا أنها لا تتمتع بقدرٍ كافٍ من الأمن.

ماذا عن الأفراد الذين يقودون هذه العملية؟ سيبقى أسانجات العالم موجودين في المستقبل، لكن قواعد دعمهم ستبقى صغيرةً. وسيكون الترحيب الأكبر من نصيب مواقع التسريبات التي تحذو حذو أشخاص مثل ألكساي نافالني، المدون الروسي والناشط في مكافحة الفساد، الذي يتمتع بتعاطف الكثيرين في الغرب. فبعد أن خاب أمله من أحزاب المعارضة الليبرالية في روسيا، أطلق نافالني، وهو محامٍ متخصص في مجال العقارات، مدونته الخاصة التي خصصها للكشف عن الفساد في الشركات الروسية الكبرى. وبدأ بتأمين التسريبات في البداية بنفسه عبر شراء أسهمٍ صغيرة في الشركات واستخدام حقوقه كصاحب أسهم لإجبارها

على مشاركته المعلومات. ثم قام بنقل أسلوبه في ما بعد، طالباً من أنصاره القيام بالمثل، ومحققاً بعض النجاح. ثم نمت مدونته لتتحول في النهاية إلى منصة كشف أسرار كاملة تحث زوارها على التبرع لتغطية تكاليف تشغيلها عبر موقع باي بال. ونما رصيد نافالني مع تنامي تشكيلة الأخبار التي لديه، والتي كان أبرزها مجموعة وثائق مسربة تكشف عن إساءة استخدام أربعة مليارات دولار ضمن شركة خطوط النفط المملوكة للدولة ترانسنفت عام 2010. وبحلول نهاية عام 2011 وصلت به مكانته العامة إلى قلب الاحتجاجات التي سبقت الانتخابات، وانتشر اللقب الذي أطلقه على حزب روسيا الموحدة لفلاديمير بوتين - أي حزب اللصوص والحرامية - كالفيروس، وصار يستخدم على نطاقٍ واسع في جميع أنحاء البلاد.

إنّ ما ميز أسلوب نافالني - على الأقل في بداية نشاطه - هو أنه في خضم حماسته لم يوجه تركيز عمليات الفضح التي يقوم بها على شخص بوتين بالذات، بل بقي يستهدف بشكل رئيس المنظمات التجارية؛ مع أن المعلومات كانت تورط بعض مسؤولي الحكومة أيضاً نظراً لصعوبة التمييز أحياناً بين القطاعين العام والخاص في روسيا. علاوة على ذلك، وبالرغم من المضايقات التي تعرض لها - حيث تم اعتقاله وسجنه والتجسس عليه والتحقيق معه في تهم اختلاس - فإنه بقي حراً على مدى سنوات. وقد ينعته ناقدوه بالكذاب أو المنافق أو العميل للسي.آي.أيه، لكن نافالني بقي في روسيا (على خلاف الكثير من معارضي الكرملين البارزين) ولم تخضع مدونته للرقابة.

يرى البعض أن نافالني لم يمثل تهديداً جدياً على الكرملين، وقد بقي الاعتراف الذي يحظى به اسمه بين الروس محدوداً جداً، مع أن مناصريه يردون بأن مثل هذه الأرقام لا تعكس سوى ضعف انتشار الإنترنت في البلاد والنجاح الذي تحققه الرقابة الحكومية على وسائل الإعلام (كان نافالني ممنوعاً من الظهور على التلفاز الحكومي). لكن نظريةً أكثر إثارةً تقول إن نافالني - في ذلك الوقت على الأقل - قد وجد طريقةً للالتزام بصفته ناشطاً ضد الفساد، فكان يعرف ما يسرّبه (ومِن مَن) والمجالات التي عليه تجنبها. وعلى خلاف المناهضين البارزين لبوتين - مثل الملياردير المعتقل ميخائيل كودوركودسكي والأوليغارشي بوريس بوريزوفسكي المقيم في منفاه الاختياري - يبدو نافالني وكأنه قد وجد طريقةً لتحدي الكرملين والاستمرار في مكافحة الفساد من دون الانجرار إلى مجالاتٍ بالغة الحساسية قد تضعه في خطرٍ جسيم. (في ما عدا صورة معالجة بطريقة رديئة ظهرت في صحيفة موالية للكرملين تظهره وهو يضحك مع بوريزوفسكي، قلما تستشعر أية صلاتٍ تربطه بالمناهضين). لقد بدا حضوره وكأنه ينال تسامحاً من الحكومة الروسية حتى تموز من عام 2012، حين وظفت جميع الوسائل المتاحة لتشويه سمعته، موجهةً له اتهاماتٍ بالاختلاس في قضيةٍ متعلقةٍ بشركة أخشاب في منطقة كيرو، حيث كان يعمل سابقاً كمستشار للحاكم. تعكس الاتهامات التي تصل عقوبتها إلى عشر سنوات في السجن مدى التهديد الذي باتت حركة الاحتجاج المرنة ضد الحكومة تشكله. وسيستمر العالم في مراقبة المسارات التي تسلكها حياة شخصيات مثل نافالني لكي يرى ما إذا كان أسلوبه يمثل إجراء حماية ناجعاً ضد الهجمات التي

يتعرض لها الناشطون الرقميون.

ثمة إمكانية مخيفة بأن تظهر مواقع ينشئها أشخاص يشاركون منصات التسريب تصميمها ومداها، لكن ليس دوافعَها، فتلعب هذه المنصات دور دار بديلة للمسربين، فتصبح مضافةً لجميع أشكال المحتوى الرقمي المختلس (كعملياتٍ عسكرية مسربة وهي قيد التنفيذ، وحسابات مصرفية مخترقة، وكلمات سر، وعناوين منـزلية مسروقة)، ومن دون أي برنامجٍ معين في ما عدا الفوضى. ولن يكون مشغلو مثل هذه المواقع إيديولوجيين أو ناشطين سياسيين، بل سيكونون عملاء للفوضى. فالمخترقون ومجرمو المعلومات ينشرون أسلابهم بلا تمييز (وقد نشرت مجموعة لولس سيك 150 ألفاً من سجلات زبائن سوني، وأتاحتها عام 2011 كملفٍ قابلٍ للتحميل عبر خدمة مشاركة ملفاتٍ متناظرة). أما في المستقبل، فإذا ظهرت منصةٌ مركزية تقدم لهم أمناً وانتشاراً على مستوى ويكيليكس، فستكون تلك مشكلةً حقيقية، ولا شك في أن مثل هذه المواقع غير المنضبطة لن تطبق الإجراءات الاحترازية التي يجريها ويكيليكس؛ كإعادة الصياغة، والتحقق مع شركائه من وسائل الإعلام (وقد أخبرنا أسانج بالفعل أنه كان يقوم بالتنقيح فقط لتخفيض الضغط الدولي الذي كان يضيق عليه مالياً، وقال إنه كان يفضل عدم إجراء أي تنقيحات). ومن الوارد جداً أن يؤدي غياب تقييم المواد الحساسة بالفعل إلى مقتل البشر. إذ إنّ مجرمي المعلومات سيمررون تسريباتٍ بالجملة بهدف إحداث أكبر قدرٍ ممكن من البلبلة؛ وهذا أمر أكيد. ويمكن القول إلى حدٍّ ما إن الانتقائية في التسريب قد تعكس هدفاً، أما إطلاق المواد بالجملة فهو عملياً ازدراءٌ لنظامٍ كاملٍ من المعلومات السرية.

لكن السياق يلعب دوره أيضاً. فكم كان رد الفعل سيختلف - تحديداً من الحكومات الغربية - لو قام ويكيليكس بنشر وثائق سرية مسروقة من أنظمة فنـزويلا وكوريا الشمالية وإيران. فلو كان برادلي مانينغ - وهو مصدر مزعوم لموادِ ويكيليكس المتعلقة بالحكومة والجيش في الولايات المتحدة - حارس حدودٍ كورياً شمالياً أو منشقاً عن قوات الحرس الثوري الإيراني، كم كانت ستختلف نظرة السياسيين والنقاد في الولايات المتحدة إليه؟ ولو قدّر لسلسلة من مواقع التسريب المخصصة للكشف عن التجاوزات داخل هذه البلدان أن تظهر، لتغيرت بالتأكيد لهجة الطبقة السياسية الغربية. فإذا أخذنا بعين الاعتبار السابقة التي قام بها الرئيس باراك أوباما في فترته الرئاسية الأولى (أسلوبٌ قاطع من عدم التهاون حيال التسريبات غير المرخّصة للمعلومات السرية من موظفي الولايات المتحدة)، فلنا أن نتوقع أن تتبنى الحكومات الغربية في المستقبل موقفاً متناقضاً حيال التسريبات الرقمية؛ مشجعةً إياها في الخارج - في البلدان المعادية - بينما تلاحقها بحزم في بلدانها.

أزمة التقارير الإخبارية

سيكون لمصادر معلوماتنا ولطريقة انتقائنا تلك الموثوقة منها أثرٌ عميق على هوياتنا في المستقبل. فما تحمله حقبة الإنترنت في جعبتها في مجال الأخبار هو

التغطية الجيدة على الأرض، في حين ستستمر المعارك التي نشهدها اليوم على استراتيجيات الإنتاج الربحي والترويج للمحتوى في العقد القادم. لكن، كيف سيتغير مشهد وسائل الإعلام كما نعرفه اليوم مع تذليل التقانة للعقبات التي تحول دون الدخول في أية صناعة؟

من الواضح تماماً أن منافذ وسائل الإعلام الرئيسة ستجد نفسها متأخرةً على نحو متزايد في مجال التقارير الإخبارية على مستوى العالم، فهذه المؤسسات عاجزةٌ ببساطة عن التحرك بسرعة كافية في عصرٍ من التواصل؛ مهما كانت موهبة المراسلين العاملين لديها أو المتعاقدين معها، ومهما توفر لها من مصادر. بدلاً من ذلك، ستستمر الأخبار الهامة في العالم بالورود من منصات شبيهة بتويتر، أي من الشبكات المفتوحة التي تسهل التشارك الفوري للمعلومات على نطاقٍ واسع وضمن حزم يتاح الوصول إليها. فإذا كان كل شخصٍ في العالم يحمل هاتفاً يدعم البيانات، أو يمكنه استخدام أحد هذه الهواتف (وهو واقعٌ ليس بالبعيد)، فإن القدرة على صنع ستبقى رهن الحظ والصدفة، وهو ما اكتشفه مدني غافل في أموتاباد في باكستان بعد أن أشار في تغريدة حية ومن دون أن يعلم عن عملية المداهمة السرية التي نالت من أسامة بن لادن[*].

في النهاية، إن فترة التأخير التي ستمر حتى تتمكن وسائل الإعلام الرئيسة من الحصول على القصة ستؤدي إلى تغير طبيعة ولاء الجمهور؛ مع سعي القراء والمتصفحين إلى الحصول على طرائق لإيصال المعلومات أكثر فورية. وسيتمكن كل جيلٍ في المستقبل من إنتاج قدرٍ أكبر من المعلومات واستهلاكه مقارنة بالجيل الذي سبقه. وسيبدي الناس قدراً أقل من الصبر إزاء وسائل الإعلام التي لا تواكب ذلك، وسينأون بأنفسهم عنها. أما ما يبقى من ولاء الجماهير فسيعود إلى التحليلات ووجهات النظر التي تقدمها هذه المنافذ، وقبل ذلك إلى الثقة التي يضعونها في هذه المؤسسات. وستنبع ثقة هؤلاء من مصداقية المعلومات، ودقة التحاليل، والأولوية التي تناط بالقصص الإخبارية. أي بعبارة أخرى، سيقسم الناس ولاءهم بين المنصات الجديدة؛ لما تقدمه لهم من ، وبين وسائل الإعلام العريقة التي تقدم لهم بقية القصة.

ستبقى مؤسسات الأخبار - بالعديد من الطرق - جزءاً هاماً لا يتجزأ من المجتمع. لكن الكثير من المنافذ لن يكتب لها البقاء ضمن شكلها الحالي. أما تلك التي ستنجو فستكون قد عدلت أهدافها وطرائقها وبنيتها التنظيمية بما يلبـي المطالب المتغيرة للجمهور العالمي الجديد. ومع انهيار الحواجز اللغوية ونهوض الأبراج الخلوية، سيظهر عددٌ غير متناهٍ من الأصوات الجديدة والمصادر المحتملة والصحفيين المواطنين والمصورين الهواة المتطلعين للمساهمة. ولا ضير في ذلك، فمع تضييق عدد كبير من المنافذ الإخبارية لمجال عملياتها؛ وخصوصاً تخفيفها أثرها على المستوى الدولي، ستبرز الحاجة إلى مثل هؤلاء المساهمين الخارجيين. وسينتفع الجمهور العالمي بدوره عبر تلقيه طيفاً أوسع من المواضيع ووجهات النظر. وسيكون لتوفر كل هذا العدد من العاملين المترابطين في ما بينهم عبر مجموعةٍ من المنصات الشبكيّة التي تشكل نظام وسائل إعلامٍ عظيماً متنافراً أثرٌ

على منافذ وسائل الإعلام الكبرى يجعلها تعمل على التحقق من المحتويات أكثر مما تعمل على إعداد التقارير.

ستصبح واجبات التقارير الإخبارية أكثر توزعاً مما هي عليه اليوم. ممّا سيؤدي إلى توسيع نطاق التغطية، لكنه ربما يخفض جودة المادة الخام. وسيصبح الدور الرئيس لوسائل الإعلام الرئيسة هو التجميع والحراسة والتحقق؛ أي إنها ستلعب دور "فلتر" المصداقية الذي يغربل كل هذه البيانات، ويسلّط الضوء على ما يستحق القراءة والفهم والثقة منها. وسيكون ما تقدمه وسائل الإعلام حاسماً بالنسبة إلى النخبة بشكلٍ خاص (أي بالنسبة إلى الزعماء التجاريين وواضعي السياسات والمثقفين الذين يعتمدون على وسائل الإعلام العريقة)، إلى جانب قدرتها على تقديم تحليلٍ مقنع. فالنخبة ستعتمد على الأرجح على مؤسسات الأخبار العريقة أكثر من غيرها، وذلك ببساطة بسبب الموجة العارمة من التقارير والمعلومات متدنية المستوى التي ستسود في النظام. فقدرة تويتر على إنتاج التحليل لا تتجاوز قدرة قردٍ على تنضيد أحد أعمال شكسبير (وإن كان تبادل تغريداتٍ ساخن على تويتر بين شخصين ذكيين يتمتعان بالمصداقية قد يوشك على الإيفاء بالغرض)؛ فقوة منصات تشارك المعلومات المفتوحة وغير المضبوطة تكمن في سرعة استجابتها، وليس في تبصرها وتعمّقها.

سيترتب على وسائل الإعلام الرئيسة إيجاد طرقٍ لدمج جميع الأصوات العالمية الجديدة التي يمكنها الوصول إليها؛ وهي مهمة صعبة ولكنها ضرورية. وستصبح مهنة الصحافة في الحالة المثالية أقل استخلاصية وأكثر تعاونية. ففي قصة عن ارتفاع مستويات المد في بانكوك، وبدلاً من مجرد الاقتباس عن ربان طوف نهري تايلندي، ستقوم الصحيفة بربط مقالتها بمنصة الأخبار الخاصة بها أو بمحطة البث المباشر، وسيزداد احتمال حدوث أخطاء عند ضم أصوات جديدة غير مدربة بالطبع؛ إذ يعتقد كثير من الصحفيين المرموقين اليوم أن ترسخ الاعتماد على صحافة المواطنين سيلحق الضرر بهذا المجال، وهي مخاوف ليست من دون مبرر.

ستقدم الاتصالات العالمية مساهمين جدداً تماماً على سلسلة التزويد، وإحدى الفئات الفرعية التي ستبرز عبارة عن شبكةٍ محلية من المختصين بالتشفير التقني الذين سيتعاملون حصراً بمفاتيح التشفير. ولن تكون قيمتهم بالنسبة إلى الصحفيين نابعةً من المحتوى، أو من طبيعة المصدر، وإنما ممّا يوفرونه من آليات السرية الضرورية بين الفرقاء. وسيكون المنشقون في البلدان القمعيّة، مثل بيلاروسيا وزيمبابوي اليوم، دائماً أكثر استعداداً لمشاركة قصصهم إذا كانوا يعلمون أنه يمكنهم القيام بذلك بأمان ومع إغفال هويتهم. وقد يكون كثيرون قادرين على تقديم هذه التقانة، لكن مختصي التشفير المحليين سيحظون بقيمة عالية نتيجة لأهمية الثقة. ولا يختلف ذلك كثيراً عما نشاهده اليوم في أنحاء الشرق الأوسط، حيث يجول متعاملون بالشبكات الخاصة الافتراضية (في.بـي.أن) الأسواق المكتظة جنباً إلى جنب مع تجار المواد المحظورة ليعرضوا على المنشقين والشباب الثوريين الاتصال من أجهزتهم بشبكة آمنة. ستعتمد مؤسسات وسائل الإعلام التي تغطي مواضيع دولية على تجار الشبكات الخاصة الافتراضية وتجار التشفير الشباب غير

المترابطين مثل اعتمادها على المراسلين الأحرار في بناء تغطيتها الإخبارية.

سيظهر نوع جديد من المراسلين الهواة أيضاً. فالشائع اليوم هو أن يكون المراسل الهاوي صحفياً غير معتمد تدفع له الصحيفة لقاء تقريرٍ. وغالباً ما يكون المراسل من بلدٍ أجنبـي أو غير مستقر. ويغامر المراسلون الهواة بأرواحهم من أجل الوصول إلى مصادر معينة، أو لزيارة مواقع خطيرة. وهم يقدمون على هذه المجازفات لأن المراسلين المحترفين لا يستطيعون أو لا يريدون التوجه إلى تلك الأماكن. وستظهر فئةٌ أخرى أيضاً من المراسلين الهواة تتألف من الرجال والنساء الذين يتعاملون حصراً بالمحتوى الرقمي والموارد الشبكية. فبدلاً من مواجهة الأخطار على الأرض سيستفيد هؤلاء من ارتفاع التواصلية العالمية لكي يعثروا على المعلومات ويشاركوها ويستخرجوها من مصادر لا يعرفونها إلا عبر الشبكة. وسيقومون بوصل الصحفيين بهذه المصادر؛ كما يفعل المراسلون الهواة اليوم. ومن الجليّ على ضوء الطبقة الإضافية التي يضفيها العالم الافتراضي من المسافة والتشويش، أنه سيترتب على منافذ وسائل الإعلام أن تتوخى قدراً أكبر من الحذر مما اعتادت عليه في مسائل الإخراج والتحقق من المصادر والأخلاقيات.

تخيل أن يقوم المشاهير في المستقبل بإطلاق بوابة أخبار خاصة بهم على الإنترنت ليتناولوا عبرها نـزاعاتٍ إثنية بعينها تثير لديهم اهتماماً عميقاً. فربما يعتقدون أن وسائل الإعلام الرئيسة لا تقوم بما يكفي للتعريف بها، أو إنها قد حصلت على الرواية الخاطئة، فيقررون تجاوز الوسطاء التقليديين وإيصال قصصهم إلى الجمهور مباشرةً. ولنُسمِّ بوابة الأخبار هذه برانجيلينا نيوز. يقوم هؤلاء باستخدام أشخاصٍ يعملون في منطقة النـزاع، ويقدمون تقارير يومية يصوغها العاملون لديهم في بلدانهم على شكل مقالاتٍ إخبارية تنشر على منصتهم. وستكون التكاليف الإضافية التي يتحملونها منخفضة؛ أقل بالتأكيد مما تتكبده منافذ الأخبار الرئيسة. بل ربما لن يكون عليهم دفع تعويضات للمراسلين المحترفين والهواة الذين سيعمل بعضهم مجاناً مقابل فرصة الظهور. وسرعان ما سيتحولون إلى المصدر الأخير للمعلومات والأخبار حول النـزاع لأنهم بارزون جداً، وقد بنوا في الوقت نفسه مصداقية في عملهم تسمح بتناولهم على محمل الجد.

ستجد منافذ وسائل الإعلام الرئيسة في المستقبل أمامها هؤلاء المنافسين الجدد (وليس فقط المغردين والمراقبين الميدانيين الهواة)، مما يجعل بيئة وسائل الإعلام معقدةً في هذه المرحلة. وكما سبق وقلنا، إنّ الكثيرين سيبقون على تفضيلهم ودعمهم لمنظمات الأخبار العريقة من باب الولاء والثقة بهذه المؤسسات. وسيبقى العمل الجاد في الصحافة، أي الصحافة الاستقصائية، والمقابلات عالية المستوى، والمسايقة المتبصرة للأحداث المعقدة، موجوداً في وسائل الإعلام الرئيسة. لكن، سيجد آخرون في تنوع موارد المحتويات فرصةً للاختيار بين مصدر جاد ومصدر من مصادر المشاهير. ويوحي هذا النهم الذي يبدو غير قابلٍ للإشباع بالمحتويات المقتضبة (في الولايات المتحدة والمملكة المتحدة وغيرها) بأن الكثير من المستهلكين سيختارون مصادر المشاهير على الأرجح، وستكون شفافية المحتوى - وليس اتساقه أو قوته - هي التي تقف وراء شهرة

أمثال أولئك الناشرين.

وتماماً كما يفعلون اليوم مع الأعمال الخيرية والمخاطرات التجارية، سينظر المشاهير إلى منافذهم الإعلامية الخاصة على أنها توسعة منطقية لعلامتهم (ونحن نستخدم هنا تعريفاً عريضاً لكلمة مشهور بأوسع معنىً ممكن. إذ نقصد به جميع الشخصيات العامة البارزة إلى حدٍّ كبير، والتي قد تشمل اليوم أي شخص، من نجوم تلفاز الواقع إلى مشاهير الخطباء الإنجيليين). ولا بد من التأكيد هنا على أن الكثير من المصادر الجديدة ستكون محاولات جادة للمساهمة في الخطاب العام، لكن الكثير منها أيضاً سيكون تافهاً وخاوياً من المحتويات تقريباً، أي إنه لن يكون أكثر من مجرد تمارين على التسويق أو الترويج للذات وتحقيق الشهرة التجارية.

سنشهد فترةً يتقاطر فيها الناس على بوابات المشاهير هذه تثميناً لجديتها، ولكي يصبحوا جزءاً من نـزعةٍ سائدة. ولن يضير أولئك الذين يبقون فيها أن يكون مستوى المحتوى والاحترافية أدنى مما تقدمه مؤسسات وسائل الإعلام العريقة. وسيشجب النقاد في مجال وسائل الإعلام هذه التغيرات وينوحون على موت الصحافة؛ لكن ذلك سيكون سابقاً لأوانه. فعندما يتغير الجمهور، يتغير معه العبء الذي يترافق مع إنتاج هذه التقارير. فإذا كان أحد مواقع المشاهير لا يؤمّن ما يكفي من الأخبار، أو يقوم بأخطاء مكشوفة باستمرار، فسيهجره الجمهور. فالولاءات في مجال وسائل الإعلام متقلبة، وهذه الحقيقة ستثبت نفسها باضطراد مع توسع هذا الميدان واكتظاظه. فإذا فقد عددٌ كافٍ من بوابات المشاهير إخلاص الجمهور وثقته، فستؤدي الهجرة الناتجة إلى العودة إلى منافذ وسائل الإعلام الاحترافية التي ستكون قد مرت بتحولاتها الخاصة في أثناء ذلك (بقيامها بالمزيد من التجميع، وتوسيع مجالها، وتسريع استجابتها). وليس كل من يغادر سيعود، كما أنه ليس كل من يهتم بوسائل الإعلام الرئيسة سيتخلى عن مصادر المعلومات المألوفة لصالح مصادر جديدة عصرية. ويبقى علينا أن نرى في النهاية مدى تأثير هؤلاء المنافسين من المشاهير على مشهد وسائل الإعلام على المدى الطويل. لكن ظهورهم كلاعبين في لعبة اجتذاب أكبر عددٍ ممكن من المستعرضين والقراء والمعلنين سيتسبب بلا شك في نشوء حراك.

لا تقتصر آثار توسع الاتصالات على التحديات التي يفرضها على منافذ وسائل الإعلام، فهو يفتح إمكانيات جديدة في ما يتعلق بدَور وسائل الإعلام بشكل أعم، وخصوصاً في البلدان التي لا تتمتع الصحافة فيها بالحرية. فأحد الأسباب التي تجعل المسؤولين الفاسدين، والمجرمين النافذين، وغيرهم من القوى سيئة النية في المجتمع، يستمرون في عملهم من دون خوف من الملاحقة يتمثل في سيطرتهم على مصادر المعلومات المحلية؛ إما مباشرة بصفتهم مالكين لها أو ناشرين فيها، أو بشكل غير مباشر عبر الترهيب والرشوة والمضايقات أو العنف. وهي الحال في البلدان ذات وسائل الإعلام المملوكة إلى حدٍّ كبير للدولة مثل روسيا، وكذلك في تلك التي تتمتع فيها العصابات الإجرامية بقدر كبير من السلطة، وتسيطر فيها على مناطق كبيرة مثل المكسيك. والنتيجة (لغياب الصحافة المستقلة) هي تراجع المحاسبة وانحسار الضغط الذي يمكن أن ينتج عن معرفة الجمهور بهذه الأخطاء

والاستعداد السياسي للملاحقة.

من شأن الاتصالات أن تساعد على تسوية هذا الخلل في السلطة بعدة طرق؛ ربما تكون أكثرها إثارةً عملية التشفير الرقمي، وما يمكن أن تقوم به بمساعدتها مؤسسات الإعلام المتخفية أو الواقعة تحت خطر. فتخيل مؤسسة غير حكومية دولية تأخذ على عاتقها مهمة تسهيل إيراد التقارير الموثوقة من الأماكن التي يصعب على الصحفي العمل فيها، أو يكون عمله فيها محفوفاً بالمخاطر. فما يميز هذه المؤسسة اليوم عن غيرها - كمجموعات الحراسة، وأصحاب وسائل الإعلام غير الربحية - يكمن في المنصة المشفرة التي ستبنيها وتنشرها لكي يتم استخدامها من قبل وسائل الإعلام داخل هذه البلدان وخارجها. ولهذه المنصة تصميمٌ مبتكر، لكنه مفاجئ في بسطاته. فلحماية شخصيات الصحفيين (المكشوفين أكثر من غيرهم في سلسلة إعداد التقرير) يتم تسجيل كل مراسل لبوابة معينة في النظام برمز مميز. وخلف هذا الرمز يتم تشفير الأسماء وأرقام الهواتف النقالة وغيرها من تفاصيل الهوية، حيث لا يتمكن من فك تشفير هذه المعلومات سوى أفراد رئيسين (وليس أي شخص في بوابة الأخبار) في المركز الرئيس الذي سيكون - وهذا أمرٌ في غاية الأهمية - خارج البلاد. أما داخل البلاد فيكون المراسلون معروفين فقط بواسطة الرمز المميز الذي سيستخدمونه لتسليم القصص، وللتفاعل مع مصادرهم ومع المحررين المحليين. في النهاية، إذا كان صحفي ما يرسل تقارير عن تجاوزات في الانتخابات في فنـزويلا على سبيل المثال (كما فعل كثيرون في تشرين الأول من عام 2012 خلال الانتخابات الرئاسية، وإن حصل ذلك من دون أن يكونوا مغفلي الهوية)، فلن يكون أمام أولئك الذين يقومون بالمهام القذرة لصالح الرئيس أية طريقة لمعرفة من عليهم أن يستهدفوا؛ لأنهم لا يستطيعون الوصول إلى معلومات المراسل. كما أنه ما من شخصٍ تعامل معه المراسل يعلم من يكون في الحقيقة. ولا تحتفظ المنافذ الإعلامية بمكاتب مادية رسمية لأنه يمكن استهدافها، ومن الضروري أن تدقق هذه المنافذ في مراسليها في البداية، لكن بعد دخول صحفيٍ إلى النظام يتم تحويله إلى محررٍ جديد (لم يسبق له أن قابله)، وتتبخر تفاصيله الشخصية في المنصة.

ستقوم المؤسسة غير الحكومية الموجودة خارج البلاد بتشغيل هذه المنصة من مسافة آمنة تسمح للمتشاركين فيها بالتفاعل بأمان وراء ستار من التشفير. وإذا كان التعامل مع المراسلين بالطرائق نفسها التي يتم بها التعامل مع المصادر السرية (بحماية هوياتهم والحفاظ على المحتويات التي يقدمونها) ليس بالفكرة الجديدة، فإن القدرة على تشفير هذه البيانات التي قد تكشف الهوية، واستخدامها على منصةٍ شبكية لتسهيل عملية جمع الأخبار مع إغفال الهوية لم يكن ممكناً قبل الآن. حيث يمكن تخزين القصص وغيرها من المواد الحساسة التي يكشف عنها الصحفيون بسهولة على مخدماتٍ خارج البلاد (أي في مكانٍ ما تحظى فيه البيانات بحمايات قانونيةٍ قوية)؛ مما سيخفف أكثر من انكشاف أولئك الذين في الداخل. وفي البداية قد تطلق هذه المؤسسة غير الحكومية منصتها كمنتج مجاني يتم تشغيله لصالح بوابات أخبار أخرى تمولها أطراف ثالثة، لكنها قد تأخذ في نهاية

المطاف جميع المنصات العاملة وتوحدها لبناء منصة عظيمة تتألف من صحفيين مغفلي الهوية من مختلف بلدان العالم. ومع أننا لسنا بالتأكيد بصدد الترويج لتحولٍ شامل نحو إغفال الهوية، فإننا نفترض في هذه الحالة أن خطورة الوضع الأمني ومدى القمع الذي يتعرض له المجتمع يجعلان هذه الحركة حلاً اضطرارياً تفرضه الضرورة. فيمكن لمحررٍ في نيويورك أن يسجل دخوله إلى المنصة، ويبحث عن مراسلٍ في أوكرانيا ليجد شخصاً ما مع سجلٍ كاملٍ لقصصه المنشورة، بل ومع اقتباساتٍ من زملاء سابقين. ومن دون أن يعرف اسم الصحفي، يستطيع المحرر أن يعتمد على القصص المتوفرة، وعلى الثقة التي يوليها للمنصة ليقرر ما إذا كان سيعمل مع المراسل أم لا، وسيكون بإمكانه طلب اتصال مشفر توفره المنصة أيضاً، مع المراسل، لكي يبدأ علاقةً معه.

لن يكون بناء نظام جمع أخبار كهذا مع إغفال هوية الجميع وتشغيله أمراً صعباً. ومع تشفير التفاصيل الشخصية للصحفيين، ولمحرريهم أيضاً، وتخزين التقارير على مخدماتٍ بعيدة، سيزداد شلل أولئك الذين يعد ظهور الصحافة المستقلة خسارةً لهم. فكيف يمكن للمرء أن ينتقم من منصةٍ إلكترونية؛ خصوصاً في عصرٍ يستطيع الجميع فيه قراءة الأخبار على الأجهزة النقالة؟ إن الاتصالات محدودة نسبياً في الأماكن التي تعاني من نقص في وسائل الإعلام الحرة اليوم. لكن، عندما يتغير ذلك، سيزداد المجال الذي تصل إليه التقارير المحلية التي تتناول مواضيع حساسة، بل إنها ستصبح عالمية. وسيضمن هذان التوجهان، أي التقارير الآمنة المدعومة بالتشفير، وتوسع قاعدة القراء بفضل التطورات في الاتصالات، أن يبقى من الممكن محاكمة المفسدين علناً على الإنترنت عبر وسائل الإعلام؛ حتى حين يكون النظام القانوني في البلاد أكثر فساداً وأقل كفاءةً من أن يلاحقهم على نحوٍ لائق. وإذا كان من الصعب جرّ جميع أمراء الحرب الناشطين في شرق الكونغو إلى محكمة الجنايات الدولية، فإن حياتهم ستصبح أكثر تعاسةً إذا قام صحفيون غير معروفي الهوية ولا يمكن الوصول إليهم بتصيد كل فعلٍ يرتكبونه وتأريخه، حيث تصل قصصهم إلى أقاصي العالم الرقمي. فأقل ما سينجم عن ذلك عندها هو أن يحجم المجرمون الآخرون - الذين قد يفكرون لولا ذلك في التعامل معهم - عن التعامل معهم، وسيرتدعون لما يستشعرونه من إشعاع رقمي يصدر عنهم. بمعنى أنهم خاضعون إلى المراقبة والتدقيق من قبل العامة على نحوٍ يجعلهم شركاء تجاريين غير مرغوبين.

عودة إلى الخصوصية: اختلاف المعنى باختلاف المواطنين

تمثل مسائل الأمن والخصوصية مسؤولية مشتركة بين الشركات والمستخدمين والمؤسسات التي تحيط بنا. حيث ينتظر من شركاتٍ مثل غوغل وأبل وأمازون وفيسبوك أن تحرس البيانات، وتحصن نظمها ضد الاختراق، وتوفر أكثر الأدوات فعالية للسماح للمستخدمين بزيادة تحكمهم بخصوصيتهم وأمنهم. لكن استغلال هذه الأدوات يعود إلى المستخدمين، ففي كل يومٍ يتقرّر فيه عدم استغلالها، ستتعرض إلى خسارة بعض الخصوصية والأمن، مع استمرار التعرية التي تتعرض

لها البيانات. ولا يمكنك افتراض وجود زر حذفٍ بسيط، فخيار حذف المعلومات هو إلى حدٍّ بعيد مجرد وهم. فمن السهل بمكان استرجاع الملفات الضائعة، ورسائل البريد الإلكتروني المحذوفة والرسائل النصيّة المحذوفة. وقلما تحذف البيانات من الحواسب، حيث تعمد نظم التشغيل إلى إزالة سجلات الملف ضمن الفهرس الداخلي فقط في حين تحتفظ بمحتويات الملف الحقيقية في مكانها؛ حتى تحتاج إلى تخصيص مساحة التخزين التي يشغلها لغاياتٍ أخرى. (وحتى بعد أن تتم الكتابة فوق الملف، يكون من الممكن أحياناً استرجاع أجزاءٍ من المحتويات الأصلية بفضل الخصائص المغناطيسية للتخزين على الأقراص، وهي مشكلة يسميها خبراء الحاسب "مغنطة البيانات"). ولن يكون من حوسبة السحابة سوى أن تعزز ديمومة المعلومات بأن تضيف طبقة أخرى من الحماية البعيدة للمستخدمين ومعلوماتهم.

صُممت آليات الاحتفاظ هذه لحمايتنا من إهمالنا في أثناء تشغيلنا للحواسب. وستزداد ثقة الناس في المستقبل بالتخزين في السحابة (كما في حالة الصرافات الآلية في المصارف)، بل وسيفضلونها على الآلات المادية، واضعين ثقتهم في الشركات التي تخزن بعض أكثر معلوماتهم حساسية، ومتجنبين المجازفة بانهيار القرص الصلب، أو سرقة الحاسب، أو ضياع المستند. ومن شأن نظام نسخ احتياطي متعدد الطبقات كهذا أن يجعل التعاملات الشبكية أكثر فعاليةً وإنتاجيةً، ناهيك عن جعلها أقل انفعالية من الناحية العاطفية.

سيكون لتخزين البيانات شبه الدائم تأثير كبير على سلوك المواطنين في الفضاء الافتراضي. فسيكون هناك سجلٌ يحوي جميع النشاطات والارتباطات الشبكية. وكل شيءٍ يضاف إلى الإنترنت سيصبح جزءاً من مخزنٍ للمعلومات الدائمة. وسيكون من الممكن دائماً أن يتعرض المحتوى الشخصي لأحدهم للنشر ذات يوم فيصبح معروفاً، سواء أكان ذلك عن طريق الخطأ أو عبر تدخل إجرامي. وسيُعتبر الناس مسؤولين عن ارتباطاتهم الافتراضية في الماضي وفي الحاضر، وهو ما يفرض المزيد من المجازفة على الجميع تقريباً بما أن شبكات الأفراد على الإنترنت غالباً ما تكون أكبر وأوسع انتشاراً من شبكاتهم المادية. وستؤثر عليهم سلوكيات أولئك الذين يعرفونهم، الحسنة منها والسيئة، إيجابياً أو سلبياً (ولن تكفي إعدادات الخصوصية الصارمة على مواقع الشبكات الاجتماعية).

سيكون هذا أول جيل من البشر يكون لديه سجل غير قابل للمحو. فقد كان بإمكان زملاء ريتشارد نيكسون ربما حذف الدقائق الثماني عشرة والنصف المسجلة والمتعلقة باختراق ووترغيت والتكتم على الأمر. لكن الرئيس الأمريكي اليوم يواجه سجلاً دائماً، يحتوي على كل رسالة بريد إلكتروني أُرسلت من جهاز بلاك بيري خاصته؛ متاحاً للعموم وفقاً لقانون السجلات الرئاسية.

بما أن ، لا تكتب أي شيء لست مستعداً لقراءته مرةً أخرى في محكمةٍ أو مطبوعاً على الصفحة الأولى في صحيفة كما يقول المثل. وسيتسع هذا المثل في المستقبل ليشتمل ليس فقط على ما تقوله وما تكتبه، بل وأيضاً على مواقع الوب التي تزورها، وعلى من تضمه إلى شبكتك على الإنترنت، وما تعبر عن إعجابك به، وما يقوم به الآخرون المرتبطون بك وما يقولونه وما

يشاركونه. سيصبح مكان تخزين المعلومات الشخصية هاجساً لدى الناس، وستظهر موجة من الشركات والأعمال التجارية الناشئة التي تعد بتقديم حلول مناسبة، بدءاً بتطبيقات من حاضرنا؛ مثل سنابتشات التي تقوم آلياً بحذف الصور أو الرسائل بعد عشر ثوان، إلى الحلول الأكثر إبداعاً التي تضيف طبقةً من التشفير مع عدادٍ تنازلي أقصر. لكن هذه الحلول ستتمكن في أحسن الأحوال من تخفيف مجازفة انتشار المعلومات الخاصة على نطاق أوسع. ومردّ ذلك جزئياً الابتكارات المضادة كالتطبيقات التي تقوم آلياً بالتقاط صورةٍ للشاشة مع كل رسالةٍ أو صورة وترسلها بسرعةٍ تسبق سرعة دماغك في أمر أصابعك بتوجيه أمرٍ للحاسب. وإذا أردنا أن نتوخى المزيد من الدقة العلمية، فإن محاولات الحفاظ على خصوصية المعلومات الشخصية ستتعرض للهزيمة دائماً أمام هجومات تستغل الثغرة المقابلة الناتجة عن حقيقة أن المعلومات لا بد من أن تشاهد في النهاية حتى يكون من الممكن استخدامها. وطالما كان ذلك صحيحاً سيبقى هناك دائماً خطر أن يقوم شخصٌ ما بأخذ صورةٍ للشاشة أو بنشر المحتوى.

عندما نكون موجودين على الوب نكون في حالة نشر تفرض علينا المجازفة بأن نتحول إلى شخصياتٍ عامة، فالأمر لا يتعلق سوى بعدد الناس الذين يولوننا اهتمامهم وبدافعهم لذلك. وإذا كان الأفراد سيبقون متحفظين بعض الشيء حيال ما يشاركونه من أجهزتهم، فسيكون من المستحيل التحكم بما يلتقطه الآخرون ويشاركونه.

ستظل ديمومة المعلومات تحدياً قاسياً في كل مكان، وبالنسبة إلى الجميع كما سبق أن قلنا. لكن نوع النظام السياسي، ومستوى سيطرة الحكومة المعنية، سيحددان إلى حدٍّ بعيد الآثار التي ستتركها هذه الديمومة على الناس. وللتمحيص في هذه الفروقات بتفاصيلها سنلقي الضوء على حالة ديموقراطيةٍ منفتحة، ثم حكمٍ فردي قمعي ودولة فاشلة.

في ديمقراطية منفتحة تقدم فيها حرية التعبير ومرونة الحكم للمواطنين حافزاً للمشاركة، سيمارس المواطنون دور القاضي وهيئة المحلفين على أقرانهم على نحو متعاظم. وسيزداد زخم التوجهات التي نشهدها اليوم مع توفر المزيد من البيانات حول كل شخص. فجميع الآراء ستجد مكاناً لها في المشهد الافتراضي الواسع. وسيشجع التحديث بالزمن الحقيقي على ظهور أوساط اجتماعية ومدنية فائقة النشاط. وسيسمح انتشار الشبكات الاجتماعية في كل مكان لأي شخص بأن يلعب دور الشخصية المشهورة، والمصور الصحفي الذي يلاحقها، والمتطفل الذي يراقبها في الوقت نفسه. وسيقوم كل شخص بإنتاج مقدار وافر من البيانات عن نفسه: ماضيه وحاضره، ما يحب وما يختار، طموحاته وعاداته اليومية. وكما هو الأمر اليوم، سيكون معظم ذلك "وفق اشتراك". بمعنى أن المستخدم سيختار بملء إرادته أن يشارك المحتويات لسبب ما، اجتماعي أو تجاري، غير معروف. لكن الاستثناءات ستبقى موجودة، فكما هو الأمر اليوم أيضاً، ستوصل الكثير من المنصات الشبكية بيانات عن نشاطات المستخدم إلى شركات وأطراف ثالثة من دون معرفة صريحة منه. وسيقوم الناس بالمشاركة أكثر مما يدركون. وستكون

هذه البيانات المتدفقة نعمة على الحكومات والشركات؛ إذ ستمكنها من الاستجابة على نحو أفضل لهموم المواطنين والزبائن، وعلى استهداف الشرائح السكانية على نحو أدق، ومع ظهور مجال التحليل التوقعي، ستمكنها من توقع ما سيحمله لها المستقبل.

كما قلنا من قبل، لم يسبق لكل هذا القدر من البيانات أن كان متاحاً أمام كل هذا العدد من الناس. سيكوّن المواطنون انطباعاتهم عن بعضهم بعضاً بناءً على مصادر دقيقة وغير دقيقة؛ بدءاً بالمصادر "الشرعية"، مثل حسابات لينكيد.إن، وانتهاء بتلك "غير الشرعية"، كتعليقات اليوتيوب الشاردة المنسية منذ زمن طويل. وسيضطر عدد غير قليل من السياسيين المرموقين إلى إلقاء السلاح حين تصبح سلوكيات الماضي الموثّقة على الإنترنت تحت الضوء من جديد في ما بعد. وبلا شك سيتكفل الوقت بترسيخ نـزعة التطبيع التي تخفف من حدة المواقف الجماهيرية تجاه خيانات القادة أو إزاء تاريخٍ من تعاطي المخدرات، فمن يمكنه نسيان تنبيه الرئيس بِل كلينتون إلى أنه "لم يستنشق"؟ ربما يتجاهل جمهور الناخبين مداخلة فضائحية، أو صورة ما للمرشّح سُجِّل عليها تاريخ يرجع إلى الفترة التي تسبق سن الثامنة عشرة. وسيصبح العامة أكثر قبولاً لطيش الشباب الموثق على الإنترنت؛ ليقطع عدة خطى نحو الأمام. لكن، ليس قبل مرور فترة مؤلمة لا بد منها. وستكون هذه، بطريقة ما، هي المرحلة المنطقية الوحيدة ضمن حقبة تتميز بغياب الأبطال. فما بدأ بإعلام الجماهير وفضيحة ووترغيت، سيتابع طريقه ليدخل العصر الرقمي الجديد الذي يمكن فيه التدقيق في قدر أكبر بعد من بيانات الأفراد التي تعود إلى كل جزء من حياتهم تقريباً. وكون البشر غير معصومين عن الخطأ خلال مراحل حياتهم سيؤمن سيلاً غير متناهٍ من التفاصيل على الإنترنت؛ ينـزع هالة الأبطال الأسطوريين عنهم جميعاً.

التحليل التوقعي مجال دراسة جديد يجمع بين الإحصاء والتنقيب عن البيانات والنمذجة الحاسوبية. وهو يعتمد في نواته على استخدام البيانات للخروج بتوقعات مفيدة حول المستقبل. فيمكن للتحليل التوقعي على سبيل المثال أن يستخدم بيانات ركاب قطارات الأنفاق في نيويورك - التي تذكر عدد الركاب - لتوقع عدد القطارات التي ستلزم في يوم معين؛ بعد أن يأخذ في عين الاعتبار المواسم والتوظيف وتوقعات حالة الطقس.

سيكون على أي شخص يسعى إلى امتهان حرفة، وخصوصاً في الصفوف القيادية، أن يفكر في ماضيه إذا أراد أن يكتب له النجاح. فهل سيهمك إذا كان طبيب العائلة يمضي عطلة نهاية الأسبوع في كتابة الخطب المعادية للمهاجرين، أو إذا كان مدرب كرة القدم الذي يدرب ابنك قد أمضى سنوات عقده الثالث وهو يعمل كدليل سياحي في الحي الأحمر في بانكوك؟ ستكون لهذا المستوى المتدرج من المعلومات عن أقراننا ورؤسائنا تبعات غير مسبوقة في المجتمع. إذ سيؤثر الماضي الموثق في حياة الكثيرين في العمل وفي الحياة اليومية، وسيمضي بعض المواطنين حياتهم كاملةً وهم في غاية الإدراك لمراحل ربما كانت هشة من حياتهم متسائلين عما قد يطفو على السطح - على الإنترنت - ذات يوم.

سيصبح التهرب من الفساد والجريمة والفضائح الشخصية في البلدان الديمقراطية أصعب في عصر من المشاركة الشاملة للمواطن. ولا شك في أنه سيتوفر للمواطنين الشكاكين الذين لا يحصى عددهم أكثر مما يلزمهم مع دخول كل هذا القدر من المعلومات المتعلقة بالأفراد - من سجلات ضريبية، وخطط رحلات، ومواقع جغرافية للهاتف (أي بيانات نظم تحديد الموقع الجغرافي التي يجمعها الهاتف النقال للمستخدم) - المجال العام. وسيعمل الناشطون مع مجموعات الرقابة والأفراد يداً بيد لمحاسبة زعمائهم، وستتوفر لديهم الأدوات الضرورية لمعرفة ما إذا كانت حكوماتهم تقول الحقيقة. وقد تتراجع الثقة الشعبية في البداية، لكنها ستنهض أقوى من سابق عهدها؛ مع إدراك الجيل التالي من القادة لهذه التطورات.

عندما يتم إدراك مدى مثل هذه التغيرات بشكل كامل، ستطالب شرائح واسعة من الشعب حكوماتها بحماية خصوصيتها الشخصية، وسيكون صوتها أعلى من أي صوت نسمعه اليوم. وإذا كانت القوانين لن تغير من ديمومة المعلومات الرقمية، فإن وجود تشريعات معقولة من شأنه أن يرسي ضوابط تضمن حداً أدنى من الخصوصية للمواطنين الذين يسعون إليها. لكن المسؤولين الحكوميين اليوم، مع بضعة استثناءات، لا يفهمون الإنترنت، لا من حيث بنيتها ولا من ناحية تعدد استخداماتها. لكن ذلك سيتغير. ففي غضون عشرة أعوام سيفهم عدد أكبر من السياسيين كيفية عمل تقانات الاتصالات، وكيفية منحها القوة للمواطنين وغيرهم من الأطراف غير الحكومية. وستتمثل النتيجة في وجود شخصيات عامة في الحكومة قادرة على إدارة مناقشات أكثر غنى بالمعلومات؛ في ما يتعلق بشؤون الخصوصية والأمن وحماية المستخدم.

أما في ديمقراطيات العالم الثالث الأحدث عهداً بالمؤسسات الديمقراطية والتقانة، فستكون التشريعات الحكومية المتعلقة بالخصوصية أكثر عشوائية. حيث سيطرأ في كل من هذه البلدان حدث معين يبرز الجوانب المعرضة للخطر بطريقة دراماتيكية تثير المطالبات الشعبية؛ على غرار ما حدث في الولايات المتحدة. فقد تم تمرير قانون فدرالي عام 1994 يمنع دوائر المركبات من مشاركة المعلومات الشخصية بعد سلسلة من عمليات إساءة استخدام هذه المعلومات، ومن بينها قتل ممثلة بارزة على يدي متطفل. وعام 1988، بعد تسرب معلومات تأجير الفيديو للقاضي روبرت بورك في أثناء عملية الترشيح للمحكمة العليا، مرر الكونغرس قانون حماية خصوصية الفيديو الذي يجرّم الكشف عن معلومات الاستئجار التي تكشف عن هوية الشخص من دون موافقة الزبون*.

مع أن كل هذه الفوضى الرقمية ستشكل إزعاجاً في المجتمعات الديمقراطية، إلاّ أنها لن تدمر النظام الديمقراطي. وستبقى المؤسسات والسياسات قائمة، وإن تعرضت لضربات خفيفة. وإذا توصلت الديمقراطيات إلى القوانين المناسبة لتنظيم التوجهات الجديدة والتحكم بها، فقد تكون النتيجة تحسناً؛ من خلال تقوية العقد الاجتماعي وزيادة الفعالية والشفافية في المجتمع. لكن ذلك سيتطلب وقتاً لأن المعايير لا تتغير بسرعة، وسيترتب على كل ديمقراطية أن تتحرك وفق وتيرتها

الخاصة.

ما من شك في أن ارتفاع إمكانية الوصول إلى بيانات الأفراد من خلال ثورة البيانات سيمنح بعض نظم الحكم الفردية أفضلية خطيرة في استهداف مواطنيها.

رغم سوء هذه النتيجة، ومع أن المرء يأمل أن يتم تخفيفها عبر التطويرات المطروحة عدة مرات في متن هذا الكتاب، فإن علينا أن نتفهم أن المواطنين الذين يعيشون في مثل هذه النظم سيترتب عليهم المزيد من النضال بعدُ من أجل خصوصيتهم وأمنهم. ومن المؤكد أن زيادة الطلب على الأدوات والبرمجيات التي تساعد المواطنين الساهرين الذين يعيشون تحت وطأة القمع الرقمي ستستنهض صناعة نامية وشرسة. هنا بالذات تكمن قوة ثورة المعلومات الجديدة هذه: أمام كل سلبية ستكون ثمة استجابة مضادة قادرة على إنتاج إيجابية راسخة. وسيكون المناضلون من أجل الخصوصية والأمن أكثر من الساعين إلى تقييدهما؛ وذلك حتى في أكثر الأماكن قمعية في العالم.

لكن النظم الاستبدادية ستخوض معركة شرسة، حيث ستعمل على تقوية ديمومة المعلومات وتدعيم سيطرتها على مزودي خدمات الإنترنت والهاتف النقال لإنتاج بيئة تسهل مهاجمتها ويعيش فيها مواطنوها. وسيكون القدر القليل من الخصوصية الذي كان متوفراً ذات يوم قد تلاشى، لأن السماعات التي يحملها المواطنون طوال الوقت ستضاعف ثغرات الرقابة التي لطالما تمنت الأنظمة وضعها في منازل الناس. ولن تحمي الحلول التقنية سوى أقلية متميزة من العارفين بالتقنية، ومؤقتاً فقط. إذ ستعمد الأنظمة إلى اختراق الأجهزة قبل بيعها، بما يمكنها من الوصول إلى ما يقوله أي شخص أو يكتبه أو يشاركه؛ سراً أو علانية. وسيكون المواطنون غافلين عن مدى إمكانية إفشاء أسرارهم الخاصة. وسيمارسون من غير قصد استخبارات على أنفسهم يمكن استغلالها؛ وخصوصاً عندما يكونون فاعلين في حياتهم الافتراضية. وستستغل الدولة ذلك للتوصل إلى استنتاجات مُدينة لهم أو لما يزمعون القيام به. وستمارس الأنظمة على مواطنيها مستوى من الاستخبارات لم يسبق لها أن وصلت إليه بالطرق غير الرقمية، وذلك نتيجة البرمجيات الخبيثة التي تطلقها الدولة، إضافة إلى الخطأ البشري. إذ سيقوم مواطنون منتظمون في شبكات - إذا مُنحوا الحوافز اللازمة من قبل الدولة - بالوشي بأقرانهم. والتقانة اللازمة لكي تنجح النظم في تجنيد كاميرات الحواسب المحمولة موجودة بالفعل، وهي قادرة عملياً على غزو منـزل أحد المعارضين من دون معرفته لتسمع وتشاهد كل شيء يقال أو يُفعل فيه.

سيكون بإمكان الحكومات القمعية أن تحدد الأشخاص الذين يملكون تطبيقات تساعد على الالتفاف على الرقابة على أجهزتهم أو في منازلهم، ليصبح حتى غير المعارضين، الذين يحاولون تحميل مسلسل السوبرانو بطريقةٍ غير شرعية، عرضةً لمزيد من التدقيق. وستتمكن الدول من تنظيم نقاط تفتيش، أو مداهماتٍ عشوائية، للبحث في أجهزة الناس عن برمجيات تشفير، أو عن وحدات خدمة وكيلة (بروكسي)، قد يؤدي وجودها لديهم إلى تحميلهم غراماتٍ، أو الحكم عليهم بالسجن، أو إلى إدراجهم في قاعدة بيانات أعداء الحكومة. وكل من يُعرف عنه أنه

قد قام بتحميل وسيلةٍ للالتفاف على الرقابة سيجد الحياة صعبةً فجأةً، فلن يتلقى قرضاً، ولن يستأجر سيارةً، ولن يتمكن من شراء شيء على الإنترنت من دون شكل من أشكال المضايقة. ويمكن لعملاء الحكومة أن يتنقلوا من صفٍ إلى صفٍ في كل مدرسة وكل جامعةٍ في البلاد ليطردوا جميع الطلاب الذين تشير فعاليات هواتفهم النقالة إلى أنهم قد قاموا بتحميل مثل هذه البرمجيات. وقد تتوسع العقوبات لتشمل شبكات أولئك الطلاب من عائلةٍ وأصدقاء؛ بما يردع الشرائح الأعرض من الشعب عن مثل هذا السلوك.

في نظم الحكم الفردية الأقل شمولية، إذا لم تقم الحكومات بالفعل بإدارة حساباتٍ رسمية "مصدقّة حكومياً" فإنها بالتأكيد ستحاول التأثير على الهويات الشبكية الموجودة والتحكم بها عبر قوانين وتقنيات مراقبة. فيمكنها تمرير قوانين تفرض احتواء حسابات الشبكات الاجتماعية على معلومات شخصية معينة مثل عنوان المنـزل ورقم الهاتف النقال؛ حيث تسهل مراقبة المستخدمين. وقد تقوم ببناء خوارزميات حاسوبية متطورة تسمح لها بالطواف على حسابات المواطنين العامة بحثاً عن حسابات لا توفر المعلومات المطلوبة أو تشارك محتويات غير مناسبة.

ثمة دول متورطة منذ الآن في مثل هذا النوع من السلوك، وإن كان ذلك سراً. فمع استمرار الثورة السورية ودخولها عام 2013 أفاد عددٌ من أعضاء المعارضة السورية وعاملي المساعدات الخارجية بتعرض حواسبهم الشخصية إلى الإصابة بفيروساتٍ حاسوبية (والكثيرون منهم لم يدركوا ذلك حتى توقفت كلمات مرورهم الشبكية عن العمل فجأةً)، وقد قام اختصاصيون في تقانة المعلومات خارج سوريا بتفحص الأقراص ليؤكدوا وجود برمجياتٍ خبيثة، هي تنويعات مختلفة على فيروسات حصان طروادة (أي البرامج التي تبدو شرعيةً لكنها خبيثةٌ في الحقيقة) فهي تسرق المعلومات وكلمات السر، وتسجل ضربات المفاتيح، وتأخذ صوراً لمحتويات الشاشة، وتحملّ برامج جديدة، وتشغل كاميرات الوب والميكروفونات عن بعد، ثم ترسل كل هذه المعلومات إلى عنوان إنترنت يعود - وفقاً لمحللي تقانة المعلومات - إلى شركة اتصالات مملوكة للدولة؛ وهي المؤسسة السورية للاتصالات. وقد وصلت برمجيات التجسس في هذه القضية عبر ملفات تنفيذية (أي إنه يجب على المستخدم أن يفتح الملف بنفسه لكي يتم تنـزيل الفيروس). لكن ذلك لا يعني أن الأفراد المستهدفين كانوا غير حريصين، فقد قامت إحدى عاملات الإغاثة بتحميل ملفٍ بدا وكأنه ارتباطٌ ميت (بمعنى أنه لم يعد يعمل) خلال محادثة على الإنترنت من أجل الحاجات الإنسانية في البلاد مع شخصٍ كانت تعتقد أنه ناشطٌ معارضٌ موثوق. وبعد المحادثة فقط علمت أنها كانت تتحدث على الأرجح مع شخصٍ من طرف الحكومة انتحل هوية المعارض، ويمتلك كلمات سرٍ مسروقة، أما الناشط الحقيقي فكان قابعاً في السجن.

سيجد الناس الذين يعيشون تحت وطأة هذه الظروف أنفسهم مضطرين للنضال وحدهم ضد فريق المطاردة التابع لحكومتهم وشركائها التجاريين الفاسدين. فما ستعجز الحكومة عن بنائه بنفسها ستعهد به إلى مزودين راغبين

بالتعاون معها. وستكتسب عبارة "شريك في الجريمة" معنىً جديداً مع هذا المستوى الجديد من المراقبة. فمجرد الظهور في خلفية صورة لشخص ما قد يصبح قضية إذا تمكنت برمجيات التعرف على الوجوه التي تستخدمها الحكومة من تحديد هوية معارض في الصورة. فالتواجد الموثق في المكان الخطأ وفي الزمان الخطأ، سواء أكان في صورة أم في تسجيل صوتي أم على عنوان إنترنت، قد يسلط على المواطنين الغافلين أضواء غير مرغوب فيها. ومع أن هذا السيناريو ليس عادلاً على الإطلاق، إلاّ أننا نخشى أنه سيحدث كثيراً جداً، وقد يحفز سلوك الرقابة الذاتية لدى بقية المجتمع.

إذا كانت الاتصالات ستمنح الدولة المزيد من القوة حين تمكنها من التنقيب في بيانات المواطنين من موقع "ذبابة على الحائط"، فإنها في الوقت نفسه ستحدّ من قدرتها على التحكم بدورة الأخبار. فوسائل حجب المعلومات والدعاية والتاريخ

ستفشل كلها في منافسة ما سيتاح أمام العامة من معلومات خارجية، وسيكون للتغطية على المعلومات مفعولٌ عكسي في مواجهة شعبٍ مطّلع ومتواصل. حيث سيكون بإمكان المواطنين التقاط الحدث ومشاركته والتعليق عليه قبل أن يتسنى للحكومة أن تقرر ما تقوله أو تفعله حياله. وبفضل الانتشار الشامل للأجهزة النقالة الرخيصة ستكون هذه التربة الخصبة للقوة موزعةً على نحوٍ عادلٍ حتى في البلدان الكبيرة. ففي الصين التي تمتلك حكومتها أحد أكثر نظم المراقبة المستخدمة اليوم تطوراً ونفاذاً، لم تنفك محاولات التغطية على القصص الإخبارية تسيء إلى الدولة عبر وقوعها المتزايد في أخطاء تتعلق بتحديد أهدافها.

ففي شهر تموز من عام 2011 أدى حادث القطار السريع في وين زو في جنوب شرق الصين إلى وفاة أربعين شخصاً، مما عزز المخاوف التي كانت محسوسةً على نطاقٍ واسعٍ بأن مشاريع البنية التحتية في البلاد تتقدم على نحوٍ سريع جداً لا يسمح بالقيام بتدقيقات السلامة المناسبة. إلا أن القنوات الرسمية قلّلت من شأن الحادث، وتم تصغير تغطيته في وسائل الإعلام عمداً، وتطلب الأمر عشرات الملايين من المداخلات على موقع ويبوز (موقع المدونات الصغرية الشبيهة بتويتر في الصين) حتى تعترف الدولة بأن الحادث كان نتيجة خطأ في التصميم وليس نتيجة طقسٍ سيئ أو انقطاعٍ في التيار الكهربائي كما أفيد قبل ذلك. علاوةً على ذلك، كُشف النقاب عن أن الحكومة قد أرسلت تعليماتٍ إلى وسائل الإعلام بعد مُضي وقتٍ قصيرٍ على الحادث تنصّ بدقةٍ على "عدم الاستفسار عن أسباب الحادث بل اعتماد تصريحات الأقسام الرسمية، ويمنع التشكيك، كما يمنع التوسع (في مواضيع إضافية)، والتخمين والنشر (لمثل هذه الأشياء) على مواقع المدونات الشخصية الصغرية". كما وجهت التعليمات إلى الصحفيين للحفاظ على خطاب مهدئ في تناول القصة: "من الآن فصاعداً يجب وصف حادث قطار وين زو ضمن إطار ". لكن، بينما التزمت وسائل الإعلام الرئيسة بهذه التعليمات، خرجت عنها المدونات الصغرية، مما أدى إلى حدث محرج للغاية بالنسبة إلى الحكومة الصينية.

ففي بلدٍ مثل الصين، تكون هذه التركيبة التي تضم مواطنين فاعلين مسلحين

بأجهزة تقانية في ظل السيطرة الصارمة للحكومة تركيبة هشّة جداَ. فإذا كانت سيطرة الدولة معتمدةً على يقينها من تحكمها المطلق في الأحداث، فإن كل حادثةٍ تزعزع هذا اليقين (أي كل خطوة عاثرة يلتقطها هاتفٌ ذو كاميرا، وكل كذبةٍ يتم فضح زيفها عبر معلوماتٍ خارجية) تزرع بذرة الشك التي تشجع المعارضة والعناصر المنشقة بين صفوف الشعب، وقد تؤدي إلى بلبلةٍ واسعة النطاق.

ربما ثمة مجموعة قليلة من الدول الفاشلة في العالم اليوم، لكنها تقدم لنا نموذجاً محيراً للطريقة التي تستطيع الاتصالات بها أن تعمل في الخواء السلطوي. بل يبدو أن الاتصالات البعيدة هي الصناعة الوحيدة القادرة على الازدهار في دولةٍ فاشلة. فقد ظهرت شركات الاتصالات في الصومال لتردم العديد من الهُوى التي خلفتها عقودٌ من الحرب والحكم الفاشل، ولتؤمن خدمات المعلومات والخدمات المالية، بل وحتى الكهرباء.

سيجد المواطنون طرقاً جديدة تمكنهم من فعل المزيد في المستقبل مع وصول فيضان الهواتف الذكية الرخيصة إلى المستخدمين في الدول الفاشلة. إذ ستساعد الهواتف على إتاحة فرص التعليم والرعاية الصحية والأمن والفرص التجارية التي لم تؤمنها حكومات هؤلاء المواطنين، وستقدم التقانة النقالة بدورها المنافذ الفكرية والاجتماعية والترفيهية التي يتوق إليها السكان الذين تعرضوا للأذية النفسية من قبل حكوماتهم. وإذا كانت الاتصالات لا تستطيع أن تعيد دولةً فاشلة إلى سابق عهدها، فإنها قادرة على تحسين أحوال مواطنيها تحسيناً هائلاً. وكما سنناقش في ما يلي، ستظهر طرائق جديدة لتسريع عملية التعافي المحلي تساعد المجتمعات على التعامل مع تحديات النـزاعات وما بعد النـزاعات (ونقصد هنا تطوراتٍ مثل بناء المؤسسات الافتراضية وقواعد بيانات اليد الماهرة في الشتات).

إلا أن حالات الخلاء السلطوي تمثل أيضاً فرصةً سانحةً لسيطرة الانتهازيين، وستكون الاتصالات في مثل هذه الحالات سلاحاً فعالاً بين أيديهم بالطريقة نفسها. إذ سيعاني المواطنون حديثو التواصل في الدول الفاشلة من جميع نقاط الضعف التي تفرضها البيانات غير القابلة للحذف، بينما لن تتاح لهم أيٌّ من الميزات الأمنية التي تحصنهم من هذه المجازفات. حيث سيجد أمراء الحرب وسالبو الأموال والقراصنة والمجرمون، إذا تمتعوا بما يكفي من الذكاء، طرقاً لتعزيز نفوذهم عبر استغلال بيانات الآخرين. وقد يعني ذلك استهداف شرائح سكانية بعينها كالأغنياء، أو القادة الدينيين ذوي النفوذ، بمزيدٍ من الدقة، وبدون أي احتمال للتعرض للمحاسبة عملياً. فإذا أظهرت بيانات الإنترنت (مثل سجلات التحويل على منصة أموال سهلة الانتقال) أن عائلةً معينةً قد تلقت مبلغاً كبيراً نسبياً من المال من أقرباء بعيدين يعيشون في بلاد الغربة، فقد تزورها عصاباتٌ محلية مطالبة بأتاوةٍ تدفع على الأرجح عبر نظام أموالٍ سهلة الانتقال أيضاً. لقد اغتنى أمراء الحرب اليوم عبر لعب دور الوسيط الذي لا غنى عنه للوصول إلى شتى أنواع الموارد القيمة، وستصبح البيانات الشخصية في المستقبل ذات قيمة؛ مثلها في ذلك مثل العقاقير والمعادن والأموال. وقد لا يستخدم أمراء الحرب في المستقبل هذه البيانات أصلاً، بل سيبيعونها إلى أطراف خارجية لا تمانع في الدفع مقابل الحصول عليها. والأهم من

ذلك أن أولئك الانتهازيين سيتمكنون من إخفاء هوياتهم ومن المراوغة أكثر مما يمكنهم اليوم لأنهم سيتمكنون لسوء الحظ من حيازة الموارد والحوافز اللازمة لتحقيق إغفال الهوية بطرق لا يستطيعها الناس العاديون.

قد يجد كثيرون في وادي السيليكون عبارات

وكأنها تنتمي إلى عالم غريب لا صلة لهم به. لكن ذلك سرعان ما سيتغير، فشركات التقانة تؤكد اليوم على تركيزها على نسخة المواطنة التي يطرحها العالم الافتراضي، وعلى مسؤوليتها عنها. ومع دخول خمسة مليارات شخص جديد إلى الشبكة، ستجد هذه الشركات أن خصائص هؤلاء المستخدمين ومشاكلهم أكثر تعقيداً بكثير مما كان للمليارين الأولين. فكثيرون من بين هذه المليارات الخمسة يعيشون تحت ظروف الفقر والرقابة وغياب الأمن. وسيتوجب على شركات التقانة، بصفتها المزود للمنصات والأدوات والاتصالات، أن تحمل بعض أعباء العالم المادي التي تفرض نفسها على الشبكة إذا كانت تريد أن تبقى وفية لمبدأ المسؤولية إزاء جميع المستخدمين.

وسيتوجب على شركات التقانة أيضاً أن تتجاوز توقعات زبائنها في مجالي الخصوصية والحماية الأمنية. وليس من المفاجئ أن معظم اللوم على التطورات غير المرغوبة في مستقبلنا سيقع على الشركات المسؤولة عن هندسة العالم الافتراضي. وسيكون بعض الغضب الذي سيصب على شركات التقانة مبرراً، فهذه الشركات ستكون في النهاية هي الرابحة من توسيع الشبكات بسرعة. لكن الكثير منه سيكون في غير محله أيضاً، فإلقاء اللوم على منتجٍ بعينه أو على شركةٍ ما بسبب تطبيقٍ معينٍ للتقانة يكون مسيئاً أسهل بكثيرٍ في نهاية المطاف من الاعتراف بقصور المسؤولية الشخصية. وستكون هناك بالطبع دائماً شركات تسمح لرغبتها في الربح بأن تطغى على مسؤوليتها تجاه المستخدمين؛ ولو كانت مثل هذه الشركات ستعاني أكثر من غيرها للوصول إلى النجاح في المستقبل.

لا شك في أن بعض شركات التقانة أكثر إدراكاً من غيرها للمسؤولية التي تحملها على عاتقها تجاه مستخدميها وتجاه الوسط الشبكي حول العالم. وهنا يكمن أحد الأسباب التي تجعل جميع المنتجات والخدمات الشبكية تقريباً تفرض اليوم على المستخدمين القبول بالشروط والبنود القانونية، والالتزام بالأدلة التعاقدية. ويتحمل الناس مسؤولية قراءة سياسات الشركة وموقفها إزاء الخصوصية والأمن قبل مشاركتهم المعلومات بملء إرادتهم. ومع استمرار تكاثر الشركات، سيتاح للمواطنين المزيد من الخيارات، لذا ستصبح اليقظة اللازمة هنا على قدر غير مسبوق من الأهمية. والمستهلك الذكي لن ينظر فقط إلى جودة المنتج، بل أيضاً إلى مدى تسهيله للتحكم بالخصوصية والأمن. لكن هذه الشروط الموضوعة مسبقاً تبقى محدودة الفعالية في محكمة الرأي العام، وفي البيئات التي يكون فيها تطبيق القانون متزعزعاً، ويمكننا أن نتوقع إيلاء المزيد من الاهتمام لمصنعي مثل هذه الأدوات ومورديها في العقود القادمة.

سيؤثر هذا التوجه بلا شك على طريقة تكوّن شركات التقانة ونموها وتحركاتها في هذه الحقبة التي ستكون عاصفة بالتأكيد. وستجد قطاعات فرعية معينة من

صناعة التقانة تتعرض لتركيز سلبـي على نحوٍ خاص صعوبةً في إيجاد مهندسين، أو في جذب المستخدمين إليها، وفي تسهيل منتجاتها؛ على الرغم من حقيقة أن مثل هذا الضمور لن يحلّ المشكلة (بل وسيمثل إيذاءً لوسط المستخدمين في النهاية عبر حرمانهم من المنافع الكاملة للإبداع). وسيكون تحمل النقد ضرورة لا غنى عنها بالنسبة إلى شركات التقانة خلال السنوات القادمة من العصر الرقمي لأنها ستجد نفسها محاصرةً بهواجس العامة إزاء الخصوصية والأمن وحمايات المستخدمين. وببساطة سيكون من المستحيل تجنب مثل هذه النقاشات، كما أن الشركات لن تتمكن من تجنب اتخاذ موقفٍ إزاء هذه المسائل.

سيتوجب على هذه الشركات أيضاً توكيل المزيد من المحامين. فوتيرة المقاضاة ستسبق دوماً الإصلاح القانوني الحقيقي. وهو ما يشهد عليه أيٌ من عمالقة التقانة الذين يخوضون معارك قانونية دائمة من أجل حقوق الملكية الفكرية وبراءات الاختراع والخصوصية وغيرها من المواضيع. فغوغل لا تنفك تتلقى دعاوى من الحكومات حول العالم - بوتيرةٍ لا يستهان بها - تتعلق بخروقاتٍ مزعومة لحقوق الملكية الفكرية أو للقوانين الوطنية. وهي تبذل قصارى جهدها لتؤكد لمستخدميها أنها تعمل لتلبية حاجاتهم والحفاظ على مصالحهم أولاً وقبل كل شيء، مع بقائها ضمن حدود القوانين. أما لو قامت غوغل بإيقاف عملية تطوير المنتج برمته كلما وجدت نفسها في مواجهة دعوى حكومية، لما تمكنت من بناء أي شيء على الإطلاق.

سيترتب على الشركات أن تتعلم كيفية التعامل مع الآمال التي تعقدها الجماهير على الإمكانيات التي تطرحها منتجاتها والمحدوديات التي تنطوي عليها. وسيكون على الشركات - على غرار الحكومات حين تضع سياساتها - أن تحلل جميع أشكال الديناميات المحلية والدولية؛ كبيئة المجازفة السياسية، والعلاقات الدبلوماسية بين الدول، والقوانين التي تحكم حياة المواطنين. ففي هذه الجلبة، ستضيع تدريجياً الحقيقة الجوهرية في صناعة التقانة، أي إن التقانة حيادية بينما الناس ليسوا كذلك. لكن تقدمنا التعاوني كمواطنين في العصر الرقمي سيتوقف على عدم نسياننا هذه الحقيقة.

استراتيجيات المواكبة

سينهض الأفراد والمؤسسات في مختلف أنحاء العالم لمواجهة التحديات الجديدة التي يواجهونها باتباع استراتيجيات مواكِبة مبتكِرة في القطاعين الخاص والعام. ويمكننا تصنيف هذه الاستراتيجيات تصنيفاً تقريبياً ضمن أربع فئات: تجارية، قانونية، مجتمعية، شخصية.

فإذا أرادت شركات التقانة تجنب التشريعات الحكومية غير المرغوبة التي قد تخنق ديناميات الصناعة، فلن يكفي أن تنهض بمسؤولياتها في مجالي الخصوصية والأمن. وقد بدأت الشركات بالفعل باتخاذ خطواتٍ وقائية مثل توفير "زر الطرد" الرقمي، الذي يسمح للمستخدمين بتحرير جميع بياناتهم من منصةٍ معينة، وإضافة مدير تفضيلات، وعدم بيع معلوماتٍ تدل على هوية الشخص إلى طرفٍ ثالث أو إلى

المعلنين. لكن المخاوف المنتشرة اليوم في ما يتعلق بالخصوصية والأمن تشير إلى وجود قدرٍ كبيرٍ من العمل لا يزال ينتظر إنجازه. وربما تتعهد مجموعةٌ من الشركات بعدم بيع بياناتٍ إلى طرفٍ ثالث ضمن معاهدةٍ تجارية أو ما شابه.

ستركز استراتيجية المواكبة الثانية على الخيارات القانونية. فعندما ينقشع الغبار عن آثار ثورة البيانات، سترزح الدول تحت ضغطٍ متزايدٍ لحماية مواطنيها من ديمومة ما يظهر على الإنترنت، ومما يظهر لديهم حديثاً من نقاط ضعف؛ الأمر الذي يعني في الديموقراطيات قوانين جديدة ستكون على الأرجح غير كاملة، ومبالغة في مثاليتها، ومتعجلةً في معظم الأحوال. لكنها ستمثل بشكلٍ عام أفضل محاولات المجتمع للاستجابة على نحوٍ فعال للتغيرات الفوضوية غير المتوقعة التي ستنجم عن الاتصالات.

كما ناقشنا سابقاً، إن تشكل ذيل المعلومات الذي سيشكل هوياتنا الشبكية في المستقبل يبدأ قبل تحصيل أي مواطنٍ للحكمة الضرورية لفهم ما يحدث. وسيتعرض الشباب خلال العقد القادم إلى قدرٍ من التدقيق لا يشبه أي شيءٍ رأيناه من قبل. فإذا كنت تعتقد أنه من الصعب النجاح في مقابلةٍ في جمعيةٍ سكنية ما اليوم، فتخيل كيف سيكون الأمر إذا كانت الهيئة تمتلك بين يديها شيئاً يشبه قصة حياتك كاملة. وبما أن هذا التطور سيؤثر على شرائح واسعة من السكان، فسيتوفر ما يكفي من الضغط الشعبـي والإرادة السياسية لإنتاج طيفٍ من القوانين الجديدة الخاصة بالعصر الرقمي.

عندما يصل الجيل القادم إلى سنّ البلوغ مع توثيقٍ رقميٍ لكل فعلٍ غير مسؤول قام به في فترة الصبا، فمن الصعب الاعتقاد بأن أياً من السياسيين سيحجم عن مناصرة قضية إغلاق السجلات الافتراضية الصبيانية. وهكذا، قد يصبح أي شيءٍ يشاركه الفرد قبل بلوغه سن الثامنة عشرة غير قابلٍ للاستخدام؛ حيث سيكون مغلقاً وممنوعاً عن الكشف العلني تحت طائلة الغرامات، بل وحتى السجن. وستجرّم القوانين النظر إلى هذا المحتوى من قبل موظفٍ أو محكمة أو إدارةٍ سكنية أو جامعة. وسيكون من الصعب بطبيعة الحال تطبيق هذه القوانين، لكن مجرد وجودها سيساهم في تغيير المعايير السائدة، حيث يُنظر إلى معظم هفوات المراهقة في النهاية من قبل المجتمع بالطريقة نفسها التي يُنظر بها إلى الأدوية التجريبية وتعاطي الممنوعات.

وقد تظهر قوانين أخرى تسعى إلى صيانة الخصوصية وزيادة الإدانة الموجهة إلى أولئك الذين يكشفون عن معلوماتٍ سرية. إذ يمكن اعتبار سرقة الهاتف الخلوي لأحدهم مكافئةً لانتحال هويته، كما قد تؤدي الاقتحامات الشبكية (كسرقة كلمات السر واختراق الحسابات) إلى تهمة الخلع والدخول عنوةً نفسها. وسيقوم كل بلدٍ بتحديد العتبة الثقافية الخاصة به التي تحدد نوع المعلومات المسموح تشاركها، والتي تميزها عن تلك التي تعتبر غير ملائمة أو شديدة الخصوصية فقط. فما تعتبره الحكومة الهندية فاضحاً أو إباحياً، ربما تمرره الحكومة الفرنسية من دون تردد. ولنفكر هنا بمجتمعٍ يبدي قلقاً عميقاً حيال مسألة الخصوصية، لكنه في الوقت نفسه مليء بالهواتف الذكية المزودة بالكاميرات وبألعاب الطائرات الرخيصة المزودة

بالكاميرات، والتي يمكن شراؤها من أي متجر ألعاب.

يمكن توسيع الفئات التي يعتمدها المصورون المتطفلون (أي الفضاء العام مقابل الفضاء الخاص) وتطبيقها على الجميع؛ مع الإشارة بوضوح إلى "نطاقات آمنة" يتطلب فيها التصوير موافقة الشخص المُصَوَّر. وسيستخدم الناس تطبيقاتٍ خاصة على هواتفهم للحصول على الإذن، فلما كانت الصور الرقمية تولد دمغةً زمنية وعلامةً مائيةً رقمية، سيكون من السهل تحديد ما إذا كان شخصٌ ما قد قام بالتقاط صورةٍ غير قانونية. والعلامة المائية الرقمية تعني إضافة بتاتٍ إلى الصورة الرقمية أو إلى ملف الصوت أو الفيديو تحتوي معلومات الحقوق الفكرية المتعلقة بمالك الملف كالاسم والتاريخ والحقوق وغيرها. وتوفر العلامة المائية حمايةً ضد التلاعب لأنها - وإن كانت غير مرئية - يمكن استخراجها وقراءتها باستخدام برمجياتٍ خاصة. فإذا اشتُبه بالتلاعب، يمكن للخبراء التقنيين تحديد ما إذا كان الملف بالفعل نسخةً غير مغشوشة أم لا.

لقد حدث بالفعل في الولايات المتحدة أن تم تطبيق قوانين الإضرار بالملكية في بعض الحالات في الفضاء السايبري.

وفي ما يتعلق بالنوع الثالث من استراتيجيات المواكبة، على المستوى المجتمعي، علينا أن نسأل أنفسنا عن الطريقة التي كان الفاعلون غير الحكوميين (كالجماعات والمنظمات غير الربحية) يستجيبون بها إزاء تبعات ثورة البيانات. ونحن نعتقد أن موجةً من المنظمات المدنية - المجتمعية ستظهر خلال العقد القادم، وستكون مصممةً لحماية المواطنين المتصلين من حكوماتهم ومن أنفسهم. ستدافع مجموعات الضغط القوية عن قوانين الخصوصية، وستنادي منظمات الحقوق التي توثّق وسائل الرقابة القمعيّة بحمايةٍ أفضل للمواطنين، وستكون ثمة مجموعات دعمٍ تساعد مختلف الشرائح السكانية على التعامل مع تبعات البيانات غير القابلة للحذف. وستحاول المنظمات التربوية الوصول إلى الأطفال في سن المدرسة لتنصحهم بتجنب المبالغة في المشاركة ("لا تعطي غريباً بياناتك أبداً"). ولنا في الحملة الأخيرة في الولايات المتحدة على البلطجة الرقمية خير نذيرٍ لما هو قادم: إدراك شعبـي واسع، وحملات توعية اجتماعية تستهدف جذور المشكلة، ومساعٍ سياسية فاترة لاحتوائها. أما في المدارس، فإننا نتوقع أن يتعامل المدرسون والإداريون مع البلطجة الرقمية بالاهتمام نفسه، وأن يفرضوا على مرتكبيها العقوبات نفسها التي يفرضونها على المشاجرات الحقيقية. وسيكون الفرق أن التلميذ سيُرسل إلى مكتب المدير ليس عند تراجع مستواه فقط، وإنما عندما يصل إلى المدرسة صباحاً، بعد أن يكون قد نشر على الإنترنت شيئاً ما في الليلة السابقة من منـزله.

إضافة إلى التخفيف من التبعات السلبية لازدياد التواصل في العالم، سيكون اللاعبون غير الحكوميين مسؤولين عن التوصل إلى الكثير من الأفكار الجديدة الواعدة التي ستقطف خير ثمار التغيرات التقنية. ففي البلدان النامية، تعمل منظمات الإغاثة منذ اليوم على تعبيد الطريق عبر مشاريع تجريبية تستفيد من الاتصالات العالمية. فخلال مجاعة عام 2011 في شرق أفريقيا أفاد مدير الوكالة

الأمريكية للتنمية العالمية راجيف شاه بأن منظمته تستخدم مزيجاً من المنصات النقالة، مع نظام تحويل الأموال التقليدي "حوالة" في الصومال لتجاوز التحريم الصارم الذي تفرضه جماعة الشباب الإسلامية على المساعدة المقدمة للشرائح السكانية المتضررة (ونظام عبارة عن شبكة من وكلاء تحويل الأموال الموثوقين تمتد عبر العالم الإسلامي وتعمل خارج المؤسسات المالية الرسمية). وقد أدى معدل النمو العالي لانتشار الهواتف النقالة والاتصالات الأساسية في البلاد إلى ظهور فرص جديدة للسكان، ولأولئك الساعين لمساعدتهم في آن معاً. وستستمر المنظمات الخيرية وغير الربحية بأداء دور خاص في التوسع في الحلول المقودة بالتقانة في العصر الرقمي الجديد. وهي في وضع ملائم جداً لأداء هذه المهمة؛ لكونها أكثر مرونة من الوكالات الحكومية، وأقدر من الشركات التجارية على امتصاص المخاطر.

نأتي الآن إلى الفئة الرابعة من استراتيجيات المواكبة وهي الفئة الشخصية، إذ سيعتمد المواطنون أكثر فأكثر على طرائق الاتصال الثنائية مغفلة الهوية. ففي عالم لا يوجد فيه زر حذف، ستصبح الشبكات الثنائية (شبكات الند للند) هي وضع العمل الافتراضي لأي شخص يسعى إلى العمل بعيداً عن الرقابة. وتسمح تقانات الند للند النقالة المعاصرة، كالبلوتوث، لجهازين ماديين بالتخاطب مباشرةً أحدهما مع الآخر، بدلاً من أن يتوجب عليهما التواصل عبر الإنترنت. وهي تختلف عن شبكات مشاركة الملفات، مثل بيت تورنت التي تعمل عبر الإنترنت. أما الأمر المشترك بين هذين الشكلين من التقانات الثنائية فهو أن المستخدمين يتواصلون في ما بينهم (أي إنهم يلعبون دور المزود والمستقبل في آنٍ معاً) من دون استخدام خدمةٍ ثابتة من طرفٍ ثالث. وستقدم الشبكات الثنائية للمواطنين في المستقبل مزيجاً مغرياً من الاتصالات الفورية والاستقلال عن سيطرة طرفٍ ثالث أو مراقبته.

تزوَّد جميع الهواتف الذكية اليوم بشكلٍ من أشكال الاتصال الثنائي. ومع إشباع الهواتف الذكية الرخيصة للأسواق الناشئة خلال العقد القادم، سيصبح بإمكان عددٍ أكبر من الناس الاستفادة من هذه الأدوات التي تزداد تطوراً. فالبلوتوث يتمتع منذ اليوم بشعبيةٍ كبيرة في الكثير من أصقاع العالم النامي لأنه يسمح حتى لأبسط الهواتف بالاستفادة منه. وفي معظم أنحاء غرب أفريقيا، حيث سبقت الهواتف النقالة في اتساعها كلاً من الحواسب والإنترنت في نموهما، يعامل الكثيرون هواتفهم وكأنها نظم "استيريو" لأن المشاركة الثنائية تسمح لهم بسهولة بتخزين الموسيقى وسماعها وتبادلها مع الآخرين عبر هواتفهم بشكلٍ كامل.

قد تكون صناديق الموسيقى النقالة في مالي استجابةً لتحديات البنى التحتية، لكن الناس في كل مكانٍ سيبدأون بتفضيل الشبكات الثنائية، وذلك لأسبابٍ شخصية في بعض الأحيان (لعدم رضاهم عن السجلات غير القابلة للحذف)، أو لأسبابٍ عملية (كالاتصالات الآمنة). ومواطنو المجتمعات القمعية يستخدمون منذ اليوم منصات الاتصال الثنائية الشائعة ونظم التراسل المشفر، مثل ريسيرتش إن موشن مراسل بلاك بيري، لكي يتفاعلوا في ما بينهم من دون خوف كبير من تدخل الحكومة. وسيحمل المستقبل معه لهؤلاء أشكالاً جديدة من التقانة التي تستخدم

نماذج الند للند، وسيضعها بين أيديهم.
تتركز النقاشات الدائرة اليوم حول التقانات القابلة للارتداء في سوق الرفاهيات: كساعات المعصم التي نرتديها لترتجّ أو تطلق نبضاً عندما يُطلق المنبه (وثمة منذ اليوم بعض النسخ منها) وأقراط الأذن التي تقيس ضغط الدم لدينا وغيره*، والتطبيقات الجديدة للواقع المدمج، أي فرض ما في العالم الافتراضي من لمسٍ وصوت وصورة على العالم المادي الحقيقي بزيادة غنى التقانة القابلة للارتداء. وقد كشفت غوغل في نيسان عام 2012 عن نموذجها الأولي للواقع المدمج باسم مشروع غلاس، وهو عبارة عن نظارة ذات شاشة داخلية أمام إحدى العينين، قادرةٌ على إيصال المعلومات ومعالجة الرسائل عبر الأوامر الصوتية، وعلى التقاط الصور، والتسجيل الفيديوي من خلال كاميرتها. وثمة أجهزةٌ مشابهة من شركاتٍ أخرى في طريقها إلينا، وسيؤدي تقاطع التقانة القابلة للارتداء مع الواقع المدمج والاتصالات الثنائية في المستقبل إلى الجمع بين البيانات الحسيّة وقنوات المعلومات الغنية والاتصالات الآمنة، وإلى إنتاج أجهزة مفيدة ومثيرة للاهتمام على نحوٍ استثنائي. ففي بلاد تجوب فيها الشرطة الدينية أو المخبرون الأماكن العامة على سبيل المثال، تصبح المعرفة بالمكان أمراً حيوياً. لذا، إن مخترع التقانة القابلة للارتداء سيصمم ساعة معصمٍ كتومة يستطيع حاملها أن يستخدمها لإرسال نبضة تحذيرٍ إلى الآخرين من حوله عندما يُلاحظ عميلاً للنظام إلى جواره. وستظهر لغةٌ غير شفوية جديدة كلياً تعتمد على البيانات الحسيّة. فقد تعني نبضتان على سبيل المثال أن عميلاً للحكومة موجودٌ في جوارك، أما ثلاث نبضات فتعني الهرب. وباستخدام معلومات نظام التموضع العالمي (جي.بـي.أس) ستقوم الساعة أيضاً بمشاركة موقع حاملها مع آخرين ربما يضعون نظارات واقعٍ مدمج قادرة على التعرف على الاتجاه الذي يأتي العميل منه. وستكون جميع هذه الاتصالات ثنائية؛ مما يجعلها أكثر أمناً وموثوقيةً مقارنةً بالتقانات التي تعتمد على الاتصال بالإنترنت.
سيعلم جهازك عن محيطك أشياء لا يمكنك معرفتها بأية طريقة: موقع الأشخاص، وهوياتهم، ومحتويات حساباتهم الافتراضية. وإذا كان المستخدمون يشاركون مكتبات آي.تيونـز التي لديهم اليوم مع الغرباء عبر شبكات واي.فاي، فإنهم في المستقبل سيكونون قادرين على مشاركة ما هو أكثر بكثير. إلا أن تقانة الاتصالات الثنائية تعتبر بديلاً محدوداً إذا قورنت بغنى الإنترنت والراحة التي تقدمها؛ وإن كانت تتمتع بميزاتٍ كثيرة. فكثيراً ما نحتاج إلى سجلاتٍ مخزنة لنشاطاتنا واتصالاتنا قابلة للبحث؛ خصوصاً إذا كنا نريد أن نشارك شيئاً ما أو أن نشير إليه في ما بعد. كما أن الاتصالات الثنائية نفسها لا تمثل لسوء الحظ تحصيناً تاماً ضد التسلل والمراقبة. فإذا استطاعت السلطات (أو المنظمات الإجرامية) التعرف على أحد طرفي المحادثة فإنها عادةً تتمكن من التعرف على الطرف الآخر أيضاً، وهو ما ينطبق أيضاً على "الدردشة" ومكالمات الصوت عبر الإنترنت (التي تجري فيها المكالمات الهاتفية عبر الإنترنت كما في غوغل فويس وسكايب)، وعلى محادثات الفيديو حيث يَفترض المستخدمون أنهم في مأمنٍ، بينما يمكن لأي شخص - إذا لم

يكن التبادل مشفراَ - أن يتنصت عليهم إذا تمكن من الوصول إلى أحد الأجزاء الوسيطة في الشبكة، حيث يقوم مهاجم - يمثل طرفاً ثالثاً في هذه الحالة - بإقحام نفسه بين المشاركين في المحادثة ونقل الرسائل بينهم من دون أن يدرك ذلك أيٌّ من المشاركين، فيلعب الطرف الثالث دور الوسيط غير المرئي الذي يخدع كل مشاركٍ ويجعله يعتقد أن المهاجم في الحقيقة هو الطرف الآخر المشارك في المحادثة. ومع جريان المحادثة (سواء أكانت نصيّة أو صوتية أو فيديوية) يمكن لهذا المهاجم الثالث أن يسترخي ويشاهد ما يجري، ليسحب من وقتٍ إلى آخر بعض المعلومات ويخزنها في مكانٍ آخر (أو يمكن للمهاجم أيضاً - إذا كان أكثر خبثاً - أن يقحم معلوماتٍ مزيفة في المحادثة). فهجومات "الوسيط" ممكنة في جميع البروتوكولات وليس فقط في حالة الشبكات الثنائية. إلا أنها تبدو أكثر خبثاً في الاتصالات الثنائية لأن من يستخدم هذه المنصات يعتقد أنه في مأمن.

وحتى إنّ الحماية التي يقدمها التشفير لا تمثل رهاناً مضموناً؛ خصوصاً إذا أخذنا بعين الاعتبار الضوابط التي ستبقى مفروضةً في العالم المادي. ففي الولايات المتحدة، سبق لمكتب التحقيقات الفدرالي وبعض المشرعين أن لـمّحوا إلى تطبيق لوائح قوانين تجبر خدمات الاتصالات مثل بلاك بيري وسكايب على الانصياع لأوامر التنصت الصادرة عن مسؤولين تنفيذيين. ويشتمل ذلك على إمكانيات اعتراض الرسائل أو تقديم المفاتيح التي تمكّن السلطات من فكّ تشفير الرسائل المشفرّة.

إن للشبكات الثنائية تاريخاً طويلاً من تحدي السلطات، خصوصاً في ما يتعلق بمواضيع الحقوق الفكرية في الديموقراطيات (مثل نابستر وبايريت باي) وفي المعارضة السياسية لأنظمة الحكم المطلقة (مثل تور). ففي الولايات المتحدة، أُغلق نابستر - الرائد في مجال مشاركة الملفات عبر تقانة الاتصال الثنائية - عام 200 عبر إنذارٍ قضائي يطلب من الشركة منع جميع التعاملات التي تشتمل على مواد محميةٍ بحقوق الملكية الفكرية على شبكتها (وقد أخبر نابستر محكمة المقاطعة أنه تمكن من منع تحويل 99.4 بالمئة من المواد المحمية بحقوق الملكية الفكرية، لكن المحكمة ردت بأن ذلك ليس جيداً بما يكفي). تقدم أجهزة بلاك بيري النقالة اتصالاتٍ مشفرة وخدماتٍ هاتفية في آنٍ معاً. وقد أدى التشفير الفريد الذي تقدمه لمستخدميها إلى جعلها عرضةً للاستهداف المباشر من قبل الكثير من الحكومات.

لن تبدي الدول القمعية الكثير من التردد في سعيها لحجب الاتصالات الثنائية أو السيطرة عليها. وسيكون على الدول الديموقراطية أن تتصرف بمزيدٍ من التأني، وقد سبق لنا أن رأينا مثالاً بارزاً على ذلك في شهر آب من عام 2011 خلال الاضطرابات في المملكة المتحدة؛ حيث احتشد المحتجون البريطانيون مطالبين بالعدالة لمارك دوغان ذي التاسعة والعشرين، والذي أصيب برصاص الشرطة البريطانية في توتنهام وقضى إثر ذلك. وبعد أيام على ذلك، تحولت الجماهير إلى العنف مضرمةً النيران في المحلات المحلية وسيارات الشرطة وحافلة، وانتشر العنف والسلب عبر البلاد خلال الليالي التالية ليصل في النهاية إلى برمنغهام وبريستول وغيرها من المدن. ونتجت عن أعمال الشغب هذه خمس وفيات،

وأضرار في الملكية قدرت بنحو 300 مليون جنيه استرليني (أي 475 مليون دولار)، وقدر كبير من الاضطراب العام. لقد كان مدى الاضطراب الذي حدث في البلاد، والسرعة التي انتشر بها، مباغتين للشرطة والحكومة. وقد اتهمت أدوات الاتصالات، مثل تويتر وفيسبوك وبلاك بيري، تحديداً بأنها أكبر العوامل العملياتية التي ساهمت بانتشار أعمال الشغب؛ مما دفع الشرطة العسكرية في توتنهام خلال أعمال الشغب إلى توجيه نداءٍ إلى بلاك بيري لإيقاف خدمة التراسل التي تقدمها خلال ساعات الليل لمنع المخلين بالأمن من التواصل. وعندما خمدت أعمال العنف، أخبر رئيس الوزراء البريطاني ديفيد كاميرون البرلمان بأنه يفكر في حجب هذه الخدمات كلياً في حالاتٍ معينة؛ خصوصاً "عندما نعلم أن هناك من يتآمر لنشر العنف والاضطراب والجريمة". وكان هدفه حسبما قال هو إما "أن يمنح الشرطة التقانة التي تمكنها من تعقب الناس على تويتر أو بـي.بـي.أم أو أن يغلقها" (وبعد اجتماعٍ مع ممثلي الصناعة، قال كاميرون إن تعاون الصناعة مع السلطة التنفيذية كان كافياً).

إن أمثلتنا عن المملكة المتحدة تنم عن وجود قلق حقيقي لدى الحكومات. لكن، من المهم توضيح أن هذا القلق كان متعلقاً بالتشفير والشبكات الاجتماعية. أما في المستقبل، فستجري الاتصالات أيضاً على شبكات ثنائية نقالة، بمعنى أن المواطنين سيتمكنون من التواصل من دون أن يضطروا إلى الاعتماد على الإنترنت (الأمر الذي لم يكن قائماً في المملكة المتحدة). ومن المنطقي أن تقوم كل الدول؛ من أقلها ديموقراطية إلى أكثرها ديموقراطية، بمحاربة نمو الاتصالات بين جهازٍ وجهاز، حيث ستدّعي الحكومات أنه في غياب القيود أو المنافذ التي يمكن استخدامها في الظروف الخاصة، سيصبح إلقاء القبض على المجرمين والإرهابيين وملاحقتهم قانونياً (وغيرها من الفعاليات الشرعية التي تمارسها الشرطة) أصعب بكثير. بينما سيصبح التخطيط للجرائم وتنفيذها أسهل بكثير. كما ستتحسن قدرة الأفراد على نشر معلوماتٍ تحتوي قدحاً وذماً أو مزيفة أو مسيئة في النطاق العام من دون محاسبة، وستخشى الحكومات الديموقراطية التشهير والتسريب غير المضبوطين، بينما ستخشى نظم الحكم المطلق المعارضين الداخليين. لكن، إذا كانت الحكومات تخشى بشكلٍ رئيس النشاطات غير القانونية، فإن التحدي الحقيقي سيكون في إيجاد مزيجٍ من العملة الافتراضية مع الشبكات مغفلة الهوية التي تخفي المواقع الفيزيائية للخدمات. فالمجرمون يبيعون منذ اليوم عقاقير غير قانونية على شبكة تور على سبيل المثال مقابل بيتكوينات (وهي عملة افتراضية) متجنبين السيولة النقدية والمصارف في آن معاً. وسيستخدم مخترقو حقوق الملكية الشبكات نفسها.

عندما نفكر في طريقة مواجهة مثل هذه التحديات، لا يمكننا أن ننظر إلى الأمر من منظار الأسود والأبيض، وللسياق دوره هنا. ففي المكسيك على سبيل المثال، يُعتبر منتجو المخدرات من بين مستخدمي التشفير مغفل الهوية الأكثر فعالية، سواء أحصل ذلك على الشبكات الثنائية أم عبر الإنترنت. وقد اجتمعنا عام 2011 ببرونو فيراري ثم بوزير الاقتصاد في البلاد الذي شرح لنا كيف تناضل الحكومة

المكسيكية من أجل إشراك الشعب في صراعها ضد المنتجين: فالخوف من العقوبة يكفي لمنع الناس من الإعلام عن الجرائم أو تزويد السلطة التنفيذية بمعلوماتٍ عن نشاطات المنتجين في أحيائهم، ثم يأتي الفساد وانعدام الثقة بقسم الشرطة ليحدّ أكثر بعد الخيارات المتاحة أمام المواطنين. "من دون إغفال الهوية"، قال لنا فيراري، "ما من آليةٍ واضحة يستطيع الناس من خلالها أن يثقوا بالشرطة ويبلغوا عن الجرائم المرتكبة من قبل منتجي المخدرات. فالإغفال الحقيقي للهوية أمرٌ جوهري لدفع المواطنين إلى المشاركة في الحل". أما منتجو المخدرات، فقد كانوا يستخدمون مسبقاً الاتصالات مغفلة الهوية، أي إن إغفال الهوية سيساوي بين الفرص المتاحة للطرفين. "والحجج التي يُدفع بها لدعم الحد من التشفير مغفل الهوية حججٌ منطقية"، يضيف لنا، "لكن، ليس في المكسيك".

الدولة البوليسية 2.0

بعد أخذ كل شيءٍ بعين الاعتبار يجد المرء أن التوازن في القوة بين المواطنين وحكوماتهم يعتمد على القدر الذي تستطيع الحكومة شراءه وتغذيته وتشغيله من تجهيزات المراقبة. وقد يترتب على الدول ذات الديموقراطيات الأصيلة أن تناضل للتعامل مع فقدان الخصوصية والسيطرة الناجمين عن ثورة البيانات. لكنها في نهاية الأمر ستحظى بمواطنين أكثر تمكناً، وبسياسيين أفضل، وبعقودٍ اجتماعية أقوى. لكن معظم دول العالم - لسوء الحظ - تكون إما غير ديموقراطية أو ديموقراطية شكلياً فقط، وسيكون الأثر النسبـي للاتصالات (الإيجابـي والسلبـي) على المواطنين في هذه البلدان أعظم بكثير مما سنشهده في أماكن أخرى.

وعلى المدى البعيد، سيؤدي حضور تقانات الاتصالات إلى تآكل الحكومات المستبدة لأن أرجحية نظام مقيد يحجب المعلومات ستتراجع باضطراد مع كل حادثٍ محرجٍ؛ لأنّ المواطنين سيكونون متمكنين ومسلحين بأجهزةٍ شخصية تدقّق في الحقائق. بعبارة أخرى، ليس من قبيل المصادفة أن الدول الاستبدادية في يومنا هذا تنتمي في معظمها إلى المجتمعات ذات المستوى الأدنى من الاتصالات في العالم. إلا أن مثل هذه الأنظمة ستكون قادرةً على المدى القصير على استغلال نمو الاتصالات لصالحها كما كانت تستغل القوانين ووسائل الإعلام. إذ يبدي الحكم المطلق نـزعةً إلى تسخير قدرات الاتصالات والبيانات بدلاً من منع تقانة المعلومات من باب الخوف؛ الأمر الذي يمثل انتقالاً من الاستبداد الصريح إلى أشكالٍ أكثر غموضاً من السيطرة يجمعها ويليام ج. دوبسون في كتابه الممتاز **منحني التعلم عند الدكتاتور**. فوفقاً لوصف دوبسون "الدكتاتوريون والمستبدون اليوم أكثر تعقيداً ومعرفةً وذكاءً مما كانوا عليه ذات يوم. فمع مواجهتهم للضغوطات المتزايدة، عمد أكثرهم ذكاءً على عدم تقسية أنظمتهم وتحويلها إلى دولٍ بوليسية، ولم ينغلقوا على أنفسهم إزاء العالم، بل قاموا بدلاً عن ذلك بالتعلم والتأقلم. وقد أدت التحديات التي فرضها تقدم الديموقراطية بالكثير من النظم الاستبدادية إلى التجريب والابتكار والمكر". ويحدد دوبسون طرقاً كثيرة

يسلكها الدكتاتوريون الحديثون لتوطيد حكمهم بينما يتظاهرون بالشرعية؛ ومنها نظام قضائي شبه مستقل، وبرلمان يوحي شكله الخارجي بأنه منتخب شعبياً، وقوانين مُصاغة صياغةً فضفاضة تُطبق اختيارياً، ومشهد من وسائل الإعلام يسمح بصحافة معارضة طالما أدرك معارضو النظام أين تقع الحدود غير المسماة. وعلى خلاف أنظمة الرجل القوي والدول المنبوذة في الماضي - كما يقول دوبسون - فإن الدول المستبدة الحديثة "مشاريع واعية مصطنعة تتطلب حرصاً في بنائها وصقلها وتقويتها".

لكن دوبسون لا يغطي سوى عدد قليل من الحالات التي يدرسها في كتابه، ونحن أقل قناعة بأن العصر الرقمي الجديد سيحمل معه مثل هذه الميزات للنظم المستبدة. وستحدد طريقة تعامل الدكتاتورات مع الاتصالات إلى حدٍّ بعيد مستقبلهم في العصر الرقمي الجديد؛ وتحديداً إذا كانت دولهم ترغب في المنافسة على الحلبة العالمية لتحقيق منـزلة أو لإجراء الأعمال التجارية. فمركزة السلطة، والموازنة الدقيقة للمحسوبيات، والقمع، والمظهر الخارجي للدولة نفسها ستعتمد كلّها على سيطرة الأنظمة على العالم الافتراضي الذي تعيش فيه شعوبها.

وخلال عقد من الزمن، سيتحول المواطنون المتصلون بالإنترنت في الأنظمة الاستبدادية في العالم من أقلية إلى أكثرية، وهو تحول مقلق بالنسبة إلى الحكام المستبدين الساعين إلى البقاء في السلطة. إلا أن بناء مثل هذا النظام القادر على مراقبة جميع أشكال الطاقة المعارضة واحتوائها ليس سهلاً لحسن الحظ، فهو يتطلب حلولاً شديدة التخصيص، ومستشارين مكلفين، وتقانات غير متوفرة على نطاق واسع، ومبالغ طائلة. إذ سيحتاج إلى أبراج خلوية ومخدمات ومكرفونات، إضافة إلى مراكز بيانات كبيرة لتخزين المعلومات. وسيكون لا بد من توفّر برمجيات مخصصة لمعالجة البيانات المجموعة، وسيقع تشغيل كل ما سبق على عاتق أشخاص مؤهلين. وسيتوجب أيضاً توفير الموارد الأساسية كالكهرباء والاتصالات توفراً مستمراً وسخياً. فإذا أراد المستبدون بناء دولة مراقبة، فإن ذلك سيكلفهم، ونأمل أن تتجاوز هذه التكلفة قدرتهم.

ثمة بعض النظم الاستبدادية التي تعاني شعوبها الفقر في بلاد تنعم بالخيرات والمعادن وغيرها من الموارد التي يمكن الاتجار بها. ويمكننا تخيل - كما في تجارة "السلاح مقابل المعادن" - نمو تبادل "التقانة مقابل المعادن" بين البلدان الفقيرة بالتقانة والغنية بالموارد (وغينيا الاستوائية هي أحد الأمثلة) والبلدان الغنية بالتقانة والمحتاجة إلى الموارد (والصين مثال واضح على ذلك). ولن يكون النجاح في هذه التجارة حليف الكثير من الدول، ونأمل أن تكون تلك التي يحالفها النجاح فعلاً غير قادرة على إدارة ما لديها وتشغيله على نحو فعال.

بعد أن توضع البنية التحتية في مكانها، ستحتاج الأنظمة القمعية إلى إدارة سيل المعلومات الذي سيجتاحها بمساعدة الحواسب المتفوقة. ففي البلدان ذات العهد الطويل بالاتصالات، كان لدى الحكومات الوقت للتأقلم مع أنواع البيانات التي ينتجها مواطنوها؛ حيث كانت وتيرة انتشار التقانة وتقدمها متدرجة إلى حدٍّ ما. أما الأنظمة حديثة الاتصال، فلن تستمتع بهذه الرفاهية، وستضطر إلى الإسراع إلى

استغلال بياناتها إذا أرادت تحقيق الفعالية في إدارتها. ولتحقيق هذا الغرض، ستقوم ببناء بنوك حاسوبية قوية مع قدرات حسابية أسرع بكثير من الحاسب الشخصي العادي. وستقوم بشراء البرمجيات التي تسهل عمليات التنقيب في البيانات والمراقبة بالزمن الحقيقي اللذين تتوق إليهما. فكل ما يحتاج إليه النظام لبناء دولة بوليسية رقمية مرعبة على نحو لا يصدق متوفر تجارياً اليوم، كما أن القيود على التصدير لا تحظى بما يكفي من المراقبة والتطبيق.

عندما يُتمّ أحد الأنظمة بناءَ دولة المراقبة، سيسارع هذا النظام إلى مشاركة ما تعلمه مع النظم الأخرى. فنحن نعلم أن الحكومات المستبدة تتشارك المعلومات واستراتيجيات الحكم والعتاد العسكري، ومن المنطقي بالتالي أن التركيبة التي تتوصل إلى تصميمها إحدى الدول ستنتشر - إذا نجحت - بين حلفائها والكثيرين غيرهم. وستقوم الشركات التي تبيع برمجيات تنقيب البيانات وكاميرات المراقبة وغيرها من المنتجات بعرض أعمالها بزهوٍّ أمام الحكومات للفوز بصفقات جديدة.

ولن تكون مداخلات الفيسبوك وتعليقات تويتر أهم أشكال البيانات التي يمكن جمعها لصالح حكمٍ مستبد، بل المعلومات البيومترية أو المقاييس الحيوية. والمقاييس الحيوية هي المعلومات التي يمكن استخدامها لتحديد هوية الأشخاص من دون شك عبر صفاتهم الجسدية والحيوية. تعتبر البصمات والصور الفوتوغرافية وفحوصات الدي.أن.أيه جميعها أشكالاً شائعة للبيانات الحيوية اليوم. وستفاجأ في المرة القادمة التي تزور فيها سنغافورة حين يطلب منك جهاز الأمن في المطار ملء استمارة الجمارك، وتسجيلاً لصوتك؛ فبرمجيات التعرف على الصوت والوجه ستتفوق في المستقبل تفوقاً كبيراً على الأشكال السابقة من حيث الدقة والاستخدام.

تستخدم نظم التعرف على الوجه اليوم كاميرا للتقريب والتركيز على عيني الفرد وفمه وأنفه لتستخرج من ذلك "مصفوفة الملامح"؛ وهي عبارةٌ عن مجموعة من الأرقام التي تصف الجوانب الأساسية في الصورة كقياس المسافة الدقيقة بين العينين (تذكر أن الصور الرقمية في النهاية مجرد أرقام). ويمكن إرسال هذه الأرقام إلى قاعدة بياناتٍ كبيرة للوجوه بحثاً عن تطابقات. وقد يرى الكثيرون في ذلك ضرباً من الخيال العلمي، والحقيقة هي أن دقة هذه البرمجيات محدودةٌ اليوم (فهي محصورةٌ مثلاً بالصورة الملتقطة من الجانب)، لكن التقدم في هذا الميدان كان لافتاً خلال السنوات الأخيرة. فقد قام فريق في كارنيغي ميلون بالولايات المتحدة عام 2011 بعرض دراسةٍ بينت أن الجمع بين برمجيات التعرف على الوجوه

والبيانات المتوفرة مشاعاً على الإنترنت قد يؤدي إلى العثور على عددٍ ضخمٍ من الوجوه بسرعةٍ كبيرة بفضل تقدمات تقنية معينة مثل الحوسبة في السحابة. وأجريت في إحدى التجارب مقارنة لصور غير معروفة الهوية من موقع للمواعدة (حيث يستخدم الناس غالباً أسماء وهمية) مع صور من حساباتٍ على مواقع الشبكات الاجتماعية التي يمكن الوصول إليها عبر محركات البحث (أي إنها لا تتطلب تسجيل الدخول)، وخرجت بنتائج هامة إحصائياً. فقد لوحظ خلال الدراسة أنه لن يكون مجدياً للإنسان أن يقوم بهذا البحث يدوياً، لكن مع حوسبة السحابة،

أصبح من الممكن مقارنة ملايين الوجوه خلال بضع ثوانٍ. وتتحسن الدقة في حال توفر الكثير من الصور للأشخاص على الإنترنت؛ الأمر الذين ينطبق في عصر الفيسبوك على الجميع عملياً.

على غرار الكثير من التطورات التقنية، يحمل عهد البيانات البيومترية الشاملة معه حلولاً مبتكرة لمشكلاتٍ اجتماعية - سياسية خانقة، وفي الوقت عينه، يجعل لعاب الدكتاتوريات يسيل. ومقابل كل نظامٍ قمعي يجمع البيانات البيومترية لكي يتمكن من اضطهاد شعبه على نحوٍ أفضل، سيوضع استثمار مشابه في بلدٍ منفتحٍ ومستقرٍ وتقدمي لكن لأسباب مختلفةٍ تماماً.

يعتبر مشروع برنامج التطابق الفريد في الهند (يو.آي.دي) أكبر مبادرة لتحديد الهوية عبر المقاييس الحيوية في العالم. وتطمح الحملة التي أطلقت عام 2009، والتي تسمى إجمالاً أدهار (بمعنى الأساس أو الدعم)، إلى تزويد كل مواطنٍ هندي (1.2 مليار والعد جارٍ) ببطاقةٍ تحتوي على معرف هويةٍ فريد من اثني عشر رقماً، زُرعت فيها شريحة حاسوبية تحتوي البيانات البيومترية للشخص؛ بما فيها بصماته ومسوحات قزحية العين. وكان يعتقد أن هذا البرنامج الضخم وسيلةٌ لحل مشكلات عدم الكفاءة والفساد والاحتيال المستشرية في النظام القائم الذي أدى تراكم التشريعات فيه إلى ما يصل إلى عشرين شكلاً مختلفاً من الهوية يتم إصدارها من قبل مختلف الوكالات المحلية والوطنية.

يعتقد كثيرون في الهند أن برنامج أدهار - خلال تقدمه - سيساعد المواطنين الذين تم إقصاؤهم من المؤسسات الحكومية وشبكات المساعدة. ويمثل أدهار بالنسبة إلى الطبقات والقبائل التي تقع تقليدياً في أسفل الهرم الاجتماعي - الاقتصادي، فرصة لتلقي مساعدات الدولة من سكن حكومي وحصص غذائية؛ وهي أشياء لطالما كانت متوفرة تقنياً، لكنها بقيت بعيدة عن متناولهم لأن الكثيرين من المتلقين المحتملين كانوا من دون هوية. أما الآخرون الذين يواجهون مصاعب في استخراج هوية، مثل العمال المهاجرين داخلياً، فسيتمكنون مع برنامج أدهار من فتح حساب مصرفي واستخراج رخصة قيادة والتقدم بطلب دعم من الحكومة والتصويت ودفع الضرائب. وعند التسجيل في البرنامج، يستطيع الفرد فتح حساب مصرفي مرتبط برقم التعريف المميز الخاص به أو بها؛ مما يمكن الحكومة من تتبع الإعانات والمنافع المحققة بسهولة.

في نظامٍ سياسي ينخره الفساد السياسي ويتخبط نتيجة حجمه (أقل من 3 بالمئة من تعداد السكان في الهند مسجلون كدافعي ضرائب)، يبدو مثل هذا المشروع واعداً، ويضمن الفوز لجميع الأطراف الشريفة. إذ سيحظى المواطنون الفقراء والريفيون بهوية، وستصبح نظم الحكومة أكثر فعالية، كما ستصبح جميع جوانب الحياة المدنية (بما فيها التصويت ودفع الضرائب) أكثر شفافيةً وشمولاً.

لكن، ثمة من يقلل من شأن أدهار، وأولئك الأشخاص يعتبرون البرنامج أورويلي* في المدى الذي يطمح إلى الوصول إليه وفي طبيعته، ويرون فيه حيلةً لتحسين قدرات المراقبة للدولة الهندية على حساب حريات الأفراد وخصوصيتهم (إذ يمكن للحكومة بالفعل استغلال أدهار لتتبع تحركات المشتبه بهم وهواتفهم ومناقلاتهم

المالية). ويشير أولئك الأشخاص أيضاً إلى أن الهنود ليسوا مضطرين لحيازة بطاقة أدهار؛ لأنه لا يحق للوكالات الحكومية المطالبة بها قبل أن تقدم الخدمات. وهذه المخاوف من تطفل الحكومة الهندية على الحريات المدنية تعيدنا بالذاكرة إلى الاعتراضات التي ظهرت على مشروعٍ مشابه في المملكة المتحدة، وهو قانون البطاقة الشخصية لعام 2006. (فبعد نضالٍ امتدَ على مدى سنواتٍ طويلة لتحقيق البرنامج، قامت حكومة الائتلاف المنتخبة حديثاً في بريطانيا بشطب الخطة عام 2010).

أما في الهند، فيبدو أن منافع المشروع تطغى بوعودها على هذه المخاوف. لكن حضورها في هذه السجالات يثبت أن الإدراك الشعبـي أو التخوف الشعبـي من أثر قواعد بيانات المقاييس الحيوية الكبيرة، وما إذا كانت ستخدم في النهاية المواطنين أم الدولة، موجودٌ حتى في الديموقراطيات. فما الذي سيحدث إذاً عندما تبدأ حكومات أقل ديموقراطية بجمع بياناتٍ بيومترية بالفعل؟ وقد بدأ الكثير منها بذلك منذ اليوم، وذلك عبر جوازات السفر.

ولن تكون الدول هي الوحيدة التي تحاول الحصول على بياناتٍ بيومترية، بل سيسعى أمراء الحرب وتجار المخدرات والمجموعات الإرهابية بدورهم إلى بناء قواعد البيانات البيومترية أو الوصول إليها؛ سعياً لتجنيد عناصر جديدة، ومراقبة الضحايا المحتملين، وإبقاء منظماتهم ذاتها تحت المراقبة. وهنا ينطبق المنطق نفسه المتعلق بالديكتاتوريات، فإذا كان لديهم ما يتاجرون به يمكنهم الحصول على التقانة.

نظراً للقيمة الاستراتيجية لقواعد بياناتٍ كهذه، يجب أن تكون الأولوية لدى الدول هي حماية معلومات مواطنيها؛ تماماً كما تحرس أسلحة الدمار الشامل. فالمكسيك في طريقها حالياً نحو نظام بيانات بيومترية يشمل سكان البلاد؛ بهدف تحسين عمل السلطة التنفيذية، ومراقبة الحدود على نحوٍ أفضل، والتعرف على المجرمين وكبار تجار المخدرات. لكن اختراق تجار المخدرات مسبقاً لقطاعات واسعة من الشرطة والمؤسسات الوطنية أنتج خوفاً حقيقياً من أن يتمكن طرفٌ غير مخول من الوصول إلى البيانات البيومترية الثمينة للشعب المكسيكي بطريقةٍ ما. وفي النهاية، ستتمكن جماعةٌ محظورةٌ ما من النجاح في سرقة قاعدة البيانات البيومترية أو الحصول عليها من الحكومة بطريقةٍ غير قانونية، وربما لن تستثمر الدول بشكلٍ كامل في إجراءات الأمن الكفيلة بحماية هذه المعلومات إلى أن يحدث ذلك.

ستتفق جميع المجتمعات على الحاجة إلى إبقاء البيانات البيومترية بعيدة عن أيدي مجموعاتٍ معينة، وستبذل جهدها لمنع المواطنين الأفراد من الوصول إليها أيضاً. وستتنوع التشريعات في هذا الخصوص؛ كما تتنوع التشريعات المتعلقة بأنواعٍ أخرى من بيانات المستخدمين. ففي الاتحاد الأوروبـي الذي يتباهى مسبقاً بسلسلة من قواعد البيانات البيومترية المتينة، يفرض القانون على الدول ذات العضوية فيه ضمان عدم انتهاك حق الفرد في الخصوصية. ويجب على الدول الحصول على موافقة المواطنين بعد إطلاعهم على المعلومات قبل أن يتم إدخال

معلوماتهم البيومترية إلى النظام؛ مما يترك للمواطنين خيار عدم الموافقة في المستقبل من دون طائلة. وعلى الدول إضافةً إلى ذلك الإصغاء إلى الشكاوى، وضمان تعويض الضحايا. وستتبنى الولايات المتحدة على الأرجح قوانين مشابهة نظراً لتقاطع المخاوف المتعلقة بالخصوصية. أما في البلدان القمعية، فمن المرجح أن تكون قواعد بياناتٍ كهذه تحت سيطرة وزارة الداخلية لضمان أن يكون استخدامها الرئيس كأداةٍ بيد الشرطة والقوى الأمنية. وسيتاح لمسؤولي الحكومة في مثل هذه الأنظمة أيضاً استخدام برمجيات التعرف على الوجه، إضافةً إلى بنوك بيانات تحتوي المعلومات الشخصية للمواطنين، وطرائق مراقبة بالزمن الحقيقي عبر الأجهزة التقانية للناس. وستجد الشرطة السرية الأجهزة الشخصية في كثيرٍ من الحالات أكثر قيمةً من السلاح.

خلال جميع المناقشات التي تتناول الخصوصية والأمن، قلما ننظر إليهما معاً ونتساءل عما يدفع الناس إلى التوتر حيال الإنترنت. فالمواطنون في العالم، سواء أكانوا في النظم القمعية أم في أكثر المجتمعات ديموقراطيةً، يخشون المجهول وما يحمله معه من أخطار وأزمات، أو يخشون أن تتشابك حياتهم في عنكبةٍ من الغرباء المتواصلين في ما بينهم، وما يحمله ذلك من مجاهيل وأخطار وأزمات. أما أولئك المتصلون مسبقاً، والذين يعيشون في عالمين مادي وافتراضي، فقد أصبح ذلك جزءاً من شخصيتهم ومن سلوكهم. ومع اعتيادنا على هذا التغير، سنتعلم أيضاً أن هذين العالمين لا يُقصي أحدهما الآخر، وإنما يتلقى كلٌ منهما تبعات ما يحدث في الآخر.

وما يتخذ اليوم شكل نقاشاتٍ دقيقة تتناول الأمن والخصوصية سيتوسع ليشمل أسئلة عن هوية من يتحكم بالهويات الافتراضية ويؤثر فيها؛ وبالتالي بالمواطنين أنفسهم. إذ ستتأثر الديمقراطيات على نحوٍ متزايد بحكمة الجماهير (بما لذلك من محاسن ومساوئ)، وستسعى نظم الحكم المطلق الفقيرة للحصول على الموارد اللازمة لتوسيع سيطرتها على نحوٍ فعال في العالم الافتراضي، بينما ستقوم الديكتاتوريات الأغنى ببناء دولٍ بوليسية حديثة تحكم قبضتها على حياة المواطنين. وستستثير هذه التغيرات سلوكياتٍ جديدة وقوانين تقدمية، لكن تعقيد التقانات ذات الصلة سيجعل المواطنين في معظم الحالات يفقدون الكثير من الحماية التي يشعرون بها ويعتمدون عليها اليوم. وستتحدد طريقة تعامل الشعوب والصناعات الخاصة والدول مع التغييرات الوشيكة إلى حدٍّ بعيد بالمعايير الاجتماعية والأطر القانونية والسمات الوطنية الخاصة.

سننتقل الآن إلى مناقشة كيفية تأثير الاتصالات العالمية على طريقة عمل الدول وتفاوضها وتصارعها في ما بينها. فلم تكن الدبلوماسية يوماً مثيرةً للاهتمام كما هي في العصر الرقمي الجديد. فالدول التي لطالما لعبت لعبة سياسات النفوذ ضمن النظام الدولي، ستجد نفسها مضطرةً إلى تعديل سياساتها الداخلية والخارجية ضمن عالم مادي وافتراضي معاً ليس من الضروري أن تنسجم فيه مصالحها دائماً.

الفصل الثالث: مستقبل الدول

ما الذي نتحدث عنه عندما نتحدث عن الإنترنت؟ إن معظم الناس ليس لديهم سوى تصور غامض لطريقة عمل الإنترنت، وهذا يكفي في معظم الحالات. فمعظم المستخدمين لا يحتاجون إلى فهم البنية الداخلية للإنترنت، أو طريقة عمل الموجهات لكي يتمكنوا من مواجهة العالم الشبكي بلا متاعب. لكننا إذا انتقلنا إلى مناقشة تأثير سلطة الدولة على الإنترنت وتأثرها بها، فإن بعض المعرفة الأساسية سيساعد على استيضاح بعض السيناريوهات المحتملة الأكثر صعوبة مفاهيمياً.

كما تم تصورها منذ البداية، تمثل الإنترنت شبكةً من الشبكات، أي شبكةً ضخمة غير مركزية من نظم الحاسب المصممة لنقل المعلومات باستخدام بروتوكولات معيارية محددة. أما ما يراه المستخدم العادي (من مواقع وب وتطبيقات على سبيل المثال) فهي بمثابة الغطاء النباتي والحيواني للإنترنت. فوراء كل ذلك تعمل الملايين من الآلات على إرسال رزم البيانات ومعالجتها واستقبالها بسرعةٍ لا تصدق عبر كابلاتٍ ألياف ضوئية ونحاسية. فكل ما نشاهده على الإنترنت، وأي شيءٍ ننتجه، يتحوّل في النهاية إلى سلسلةٍ من الأرقام التي تحزم معاً وترسل عبر سلسلةٍ من الموجّهات المتوضعة في أماكن مختلفة من العالم، ثم يعاد تجميعها على الطرف الآخر. كثيراً ما وصفنا الإنترنت بأنها فضاء ، غير محكوم وغير قابل للحكم بتصميمه. فهي بنية غير مركزية من الارتباطات المتقلبة باستمرار، والتي تجعل أية محاولةٍ من قبل الحكومة للسيطرة عليها ضرباً من العبث. لكن الدول تتمتع بقدر هائل من السلطة على آلات الإنترنت العاملة في بلادها. فنظراً للسلطة التي تمتلكها الدول على البنية التحتية المادية التي تتطلبها الاتصالات (كأبراج النقل والموجهات والمقاسم)، فإنها تتحكم أيضاً بنقاط الدخول والخروج والنقاط الوسيطة التي تمرّ بها بيانات الإنترنت. وهي قادرة على الحدّ من المحتويات، والسيطرة على التجهيزات التي يُسمح للناس باستخدامها، بل وإنتاج شبكات إنترنت منفصلة. فالدول تستمد سلطتها من الاتصالات، وكذلك المواطنون؛ لكن ليس بالطريقة نفسها. فتمكين الناس يأتي مما يتاح لهم الوصول إليه، أما الدول فتستقي نفوذها من موقعها كحارس.

لقد ركزنا حتى الآن بشكلٍ رئيس على ما سيحدث عندما ينضم مليارات البشر إلى الإنترنت (أي كيفية استخدامهم الإنترنت، وأنواع الأجهزة التي سيستخدمونها، وكيفية تغيّر حياتهم) لكننا لم نقل بعد كيف ستكون الإنترنت لديهم، أو كيف ستستغل الدول أكبر قدرٍ منها في تعاملاتها المادية والافتراضية مع الدول الأخرى ومع شعوبها بالذات. وستكون لهذه المسألة أهمية متزايدة مع ازدياد تواصل شعوبٍ تختلف في أبجدياتها ومصالحها ومعاييرها. كما أنّ كلاًّ من حكومات هذه الشعوب لديها مصالحها وضغائنها ومواردها أيضاً، وربما كان أهم سؤالٍ سيشغلنا على مدى السنوات العشر القادمة لا يتعلق باستخدام المجتمع للإنترنت أو لا، بل بالنسخة التي يستخدمها منها.

مع تأقلم المزيد من الدول مع تواجد شرائح أكبر من سكانها على الإنترنت، ستبذل هذه الدول جهدها للحفاظ على سيطرتها، سواء أكان ذلك داخلياً أم على الساحة الدولية. وستخرج بعض الدول من هذا الانتقال إلى العصر الافتراضي وقد ازدادت قوة (أي أصبحت أكثر أمناً وتتمتع بمزيد من النفوذ) مستفيدة من تحالفات قوية واستخدامات ذكية للطاقة الرقمية. بينما سيترتب على دول أخرى أن تناضل لمجرد مواكبة التغيرات التقانية والتأقلم معها محلياً ودولياً. وستمتد الصداقات والتحالفات والعداوات بين الدول إلى العالم الافتراضي؛ مضيفة بعداً جديداً محيراً لفن السياسة التقليدي. وسينظر إلى الإنترنت في النهاية، بالعديد من الطرق، كتجسيد لنظرية العلاقات الدولية الكلاسيكية التي تتحدث عن عالم فوضوي لا قيادة له. وسنبيّن في ما يلي كيفية استجابة الدول - وفق اعتقادنا - في ما بينها وتجاه مواطنيها.

بلقنة الإنترنت

كما سبق وقلنا، إنّ كل دولةٍ - وكلّ مجتمعٍ - في العالم لديها قوانينها الخاصة ومعاييرها الثقافية وسلوكياتها التي تتقبلها. ومع دخول المليارات من البشر إلى الإنترنت خلال العقد القادم، سيعيد الكثيرون منهم اكتشاف الاستقلال (في الأفكار والكلام والحديث)، وسيمثل ذلك امتحاناً لهذه الحدود الفاصلة. لكن حكومات هؤلاء المستخدمين ستفضل في معظم الأحيان أن يجد هؤلاء المستخدمون أمامهم عالماً افتراضياً يسمح للقوى الحاكمة بأن تعكس سيطرتها المادية في هذا العالم؛ وهي فكرة مفهومة وإن كانت ساذجة في أساسها. إذ ستحاول كل دولة تنظيم الإنترنت وتشكيلها وفقاً لصورتها هي.

تسود الدول - سواء أكانت تلك الديموقراطية منها أم الاستبدادية - نـزعةٌ إلى تسليط قوانين العالم المادي على العالم الافتراضي. فما تعجز الدول عن بنائه في الواقع، تحاول تفصيله في الفضاء الافتراضي؛ مقصية تلك العناصر من المجتمع التي لا تحبذها والمحتويات التي تتعارض مع قوانينها وأية تهديدات أخرى تراها. ويواجه معظم مستخدمي الإنترنت في العالم شكلاً ما من أشكال الرقابة (وإن كانت تُجمّل بتسميتها فلترة)، لكن شكلها الحقيقي يعتمد على سياسات البلد وبنيته التحتية التقانية. وليست كل فلترةٍ رقابةً سياسية، فالبلدان المتقدمة تحجب بشكلٍ روتيني عدداً متواضعاً من المواقع.

في بعض البلدان، توجد نقاط دخول عديدة للوصول إلى اتصالات الإنترنت تسيطر عليها مجموعة من شركات الاتصالات الخاصة (مع بعض التشريعات المطبقة عليها). بينما توجد بلدان أخرى ليس فيها سوى نقطة وصولٍ واحدة ومزودِ خدمة إنترنت وطني واحد تمر عبره جميع الاتصالات. وتكون الفلترة سهلةً نسبياً في الحالة الأخيرة، بينما تصعب قليلاً في الحالة الأولى. وهذه الفروقات في البنية التحتية، إضافةً إلى الخصوصيات الثقافية، والأهداف من الفلترة، تفسر عملية الترقيع في الأنظمة الجارية في العالم اليوم.

تجري الفلترة في معظم البلدان على مستوى مزود خدمة الإنترنت. وتضع

الحكومات عادةً قيوداً على موجهات البوابة التي تصل البلاد ومخدمات أسماء النطاق (دي.أن.أس) مما يسمح لها إما بحجب الموقع نهائياً (مثل موقع يوتيوب في إيران) أو معالجة محتويات الوب عبر "التفتيش العميق في الحزمة". فمع التفتيش العميق في الحزمة تسمح برمجيات متخصصة للموجِّه بالنظر إلى محتويات حزم البيانات التي تمر به، والبحث عن كلمات ممنوعة أو أشياء مشابهة داخل الحزمة (استخدام برمجيات تحليل الرأي لفرز العبارات السلبية التي تتناول سياسيين على سبيل المثال)، لتعمد إلى حجبها لاحقاً. وكلتا التقنيتين لا تعتبران سهلتين، حيث يستطيع المستخدمون الوصول إلى المواقع المحجوبة باستخدام تقانات التحايل مثل مخدمات البروكسي (التي تخدع الموجهات)، أو باستخدام بروتوكولات تشفير أتش.تي.تي.بـي.أس التي تمكن من إجراء اتصالات إنترنت خاصة لا يمكن لأي شخصٍ قراءتها، نظرياً على الأقل، باستثناء حاسبك وموقع الوب الذي تتصفحه. أما التفتيش العميق في الحزمة فنادراً ما يتمكن من التقاط كل حالات المحتويات الممنوعة. وتستثمر الدول الأكثر تطوراً من ناحية الرقابة في بناء مثل هذه النظم، وستنـزل بأولئك الذين يحاولون الالتفاف عليها عقوبات صارمة.

فعندما بدأ المختصون بالتقانة بملاحظة سعي الدول إلى تشريع نفوذها وإسقاطه على الإنترنت، حذر بعضهم من ، حيث تؤدي الفلترة الوطنية وغيرها من القيود إلى تحويل ما كان ذات يومٍ شبكة إنترنت عالمية إلى سلسلة من الشبكات التابعة للدول القومية*. وعندها ستتمزق شبكة الوب العالمية وتتشظى، وسرعان ما ستصبح هناك و وهلم جرًّا، تتعايش جميعها معاً. وقد تتقاطع أحياناً لكنها منفصلة في جوانب هامةٍ؛ حيث ستكون لكل إنترنت تابعة لدولة ما خصائصها الوطنية. وسيكون جلَّ تدفق المعلومات ضمن البلدان، وليس في ما بينها، وذلك نتيجة الفلترة واللغة، بل وحتى تفضيلات المستخدمين (ثمة أدلةٌ تبين أن معظم المستخدمين يميلون إلى البقاء في نطاقاتهم الثقافية عندما يكونون على الإنترنت؛ ليس نتيجةً للرقابة بقدر ما هو نتيجةٍ للغة المشتركة والاهتمامات الشائعة والراحة. وقد تكون تجربة التصفح أسرع أيضاً مع وجود خابية الشبكة التي تخزن المحتويات مؤقتاً على مركز بياناتٍ محلي مما يزيد سرعة وصول المستخدمين إلى المحتويات زيادةً كبيرة). وهي عمليةٌ بالكاد سيدركها المستخدمون في البداية، لكنها سرعان ما ستتبلور مع الوقت لتصبح في النهاية سمة من سمات الإنترنت.

إن المرحلة الأولى من هذه العملية، أي الفلترة العدوانية التمييزية، جاريةٌ اليوم على قدمٍ وساق، ومن المرجح جداً أن يحدث السيناريو السابق بشكل معدل، لكن درجته ستتحدد بشكلٍ كبير بما سيحدث خلال العقد القادم مع اتصال دول جديدة، أي حسب المسار الذي ستختاره تلك الدول؛ ووفقاً لمن يناهضها أو يتعاون معها، أو وفقاً للمبادئ التي يبدو أنها تسترشد بها. وللتوسع في هذه التنويعات، سنلقي نظرةً على الأساليب المختلفة للفلترة المطبقة في العالم اليوم، وقد استطعنا التعرف على ثلاثة نماذجٍ منها على الأقل: الأسلوب الفاضح، والأسلوب الخجول، والأسلوب المقبول سياسياً وثقافياً.

لا نقصد هنا شبكات الإنترانيت، فالإنترانيت تستخدم تقانة بروتوكولات الإنترنت نفسها، لكنها محصورة بشبكة تقع داخل حدود منظمة أو منطقة محلية، وهي ليست شبكة من شبكات أخرى. وغالباً ما تكون شبكات الإنترانيت التجارية محصنة ضد الوصول الخارجي غير المخول عبر جدران نارية أو غيرها من الآليات التي تطبق على البوابة.

لنبدأ بالأسلوب الفاضح، إذ تعتبر الصين أكثر البلدان المفلترة للمعلومات في العالم فعالية وحماسة، فثمة منصات تتمتع بشعبية هائلة في مناطق أخرى من العالم - مثل فيسبوك وتامبلر وتويتر - محجوبةٌ برمتها من قبل الحكومة الصينية. وثمة مصطلحات بعينها، مثل فالون غونغ (وهو اسم مجموعة روحية ممنوعة في الصين مرتبطة بأحد أجنحة المعارضة) نجدها ببساطة غائبةً في الفضاء العام الافتراضي للبلاد، بعد أن أصبحت ضحية الرقابة الرسمية أو الرقابة الذاتية واسعة الانتشار. فعلى الإنترنت الصينية لن تتمكن من إيجاد معلومات عن مواضيع حساسة سياسياً، مثل احتجاجات ساحة تيانانمن أو أية معلومات قد تحرج القيادة السياسية الصينية؛ كحركة الحقوق التيبيتية والدالايلاما، أو أية محتويات متعلقة بحقوق الإنسان والإصلاح السياسي أو مواضيع السيادة. فعندما يتعلق الأمر بأحد هذه المواضيع، تقع حتى أشهر منافذ الأخبار الغربية ضحيةً للرقابة. فقد حجبت أخبار بلومبيرغ باللغتين الإنكليزية والصينية عقب كشفها في حزيران من عام 2012 عن الثروة الطائلة التي تمتلكها عائلة شي جين بينغ الذي كان يومها نائباً للرئيس (وهو الرئيس اليوم). وبعد ذلك بأربعة أشهر كان على نيويورك تايمز أن تواجه مصيراً مشابهاً بعد نشرها قصة مشابهة حول جين وين جياباو رئيس الوزراء في ذلك الحين، وليس من المفاجئ أن أية معلوماتٍ تتناول أدوات التفاف على الرقابة محجوبة بدورها، وقد أدركنا مدى شمول سلطات الرقابة الصينية ودقتها بعد زيارةٍ إشكالية لرئيس إدارة غوغل إيريك إلى بكين عام 2011، حين اختفت جميع الآثار التي تشير إلى زيارته من الإنترنت الصينية، بينما كانت تغطية وسائل الإعلام للرحلة لا تزال موجودةً ومتاحةً في كل مكانٍ آخر.

تبقى هذه الرقابة بالنسبة للمستخدم الصيني العادي غير ملحوظة، فمن دون معرفةٍ سابقة بالأحداث أو الأفكار ستبدو هذه الأخيرة وكأنها غير موجودة أصلاً. وما يعقد الأمر أكثر بعد هو أن الحكومة الصينية لا تترفع عن إبداء قدرٍ أكبر من المبادرة حين يتعلق الأمر بمحتوى الإنترنت: إذ يقترح أحد تقديرات عام 2010 أن المسؤولين الصينيين قد وظفوا قرابة 300 ألف "معلق على الإنترنت" لكتابة مداخلاتٍ تمجد رؤساءهم في الحكومة والحزب الشيوعي (غالباً ما يدعى مثل هذا النشاط بالتعشيب الصناعي؛ أي المشاركة المزيفة للقواعد الشعبية، وهو تكتيكٌ شائع بين شركات العلاقات العامة ووكالات الإعلان والحملات الانتخابية حول العالم).

لا تتردد القيادة الصينية في الدفاع عن سياسات الرقابة الصارمة التي تتبعها. ففي تقرير حكومي رسمي أُصدر عام 2010 تسمي الحكومة الإنترنت "تبلور الحكمة البشرية"، بينما تصرح بأن لدى الصين "من القوانين والتشريعات ما يحظر صراحةً انتشار المعلومات ذات المحتويات التي تمسّ بسلطة الدولة، أو تقوضّ

الوحدة الوطنية، أو تنتهك شرف الأمة أو مصالحها". فالجدار الناري الصيني العظيم، وهو الاسم الذي تعرف به مجموعة أدوات الحجب التي تستخدمها الدولة، ليس سوى حارس على بنية الدولة الصينية. "تخضع الإنترنت على الأراضي الصينية للسلطة القضائية التي تمثل السيادة الصينية، وسيادة الصين في الإنترنت يجب أن تحترم وتُحمى". هذه الطريقة التي لا تعرف الخجل أو الاعتذار في تطبيق الرقابة ستجتذب بشكل طبيعي الدول ذات النـزعات التسلطية القوية، إضافةً إلى الدول ذات الشعوب المتجانسة أو الحساسة على نحو خاص (أي الشعوب التي تخشى من غزو المعلومات الخارجية على المستوى العاطفي).

نأتي الآن إلى مفلتري الإنترنت الخجولين، فقد اتبعت تركيا أسلوباً أكثر مكراً مقارنةً بالصين، بل إنها أبدت سرعة في الاستجابة للمطالب الشعبية بحرية الإنترنت، لكنها مع ذلك مستمرةٌ في تطبيق سياسات رقابية على الإنترنت مع قدر كبير من التعمية. وقد كانت للحكومة التركية علاقةٌ صعبة مع انفتاح الإنترنت، فهي أكثر تسامحاً بكثير من بعض جيرانها الإقليميين، لكنها أكثر تشدداً بكثير من حلفائها الأوروبيين. فمن المستحيل الحصول على اتصال إنترنت غير مفلترة أبداً في تركيا (وهو فرق هام بين تركيا والبلدان الغربية). حيث تعرَّض موقع يوتيوب للحجب من قبل السلطات التركية لأكثر من عامين بعد رفض الشركة إزالة فيديوهات ادعى المسؤولون الأتراك أنها تشوه صورة مؤسس البلاد مصطفى كمال أتاتورك (وانصياعاً لقانون يعود لعام 1951 تجرمّ أية إهانة علنية لأتاتورك، وافق يوتيوب على حجب الفيديوهات عن الجمهور التركي، لكن الحكومة كانت تريد إزالتها من المنصة على مستوى العالم). وإذا كان هذا الحجب فجّاً للغاية، فإن الرقابة التي تليه كانت أكثر كتماناً: فقد حجب نحو 8000 موقع وب في تركيا من دون أي إشعار علني أو تأكيدٍ رسمي من الحكومة.

يشيع النموذج الخجول بين الحكومات التي تناضل لتحقيق توازنٍ بين عقائد ومواقف ومخاوف متضاربة لدى شعوبها. لكن الحكومة حين تتبع هذا المسار، قد تتحول بنفسها إلى عدو إذا بالغت في مضيها فيه، أو إذا انكشفت آليات مكائدها. ولنأخذ هنا مثالاً حديثاً من تركيا، ففي عام 2011 أعلنت الحكومة سياسة فلترةٍ جديدة للإنترنت على مستوى البلاد تعتمد على نظام رباعي الطبقات للرقابة يسمح للمواطنين باختيار مستوى الفلترة الذي يرغبون به (هذه المستويات، من الأشد صرامةً إلى الأقل صرامةً، هي: مستوى الطفل، العائلة، المستوى المحلي، المستوى المعياري). وقالت هيئة تقانات الاتصالات والمعلومات (المعروفة بالتركية بحروفها الأولى بـي.تي.كي) إن الغرض من هذا البرنامج هو حماية القاصرين، ووعدت بأن من سيختار المستوى المعياري فلن يخضع لأية رقابة. لكن الكثير من المتشككين نتيجة تاريخ الهيئة في مجال الشفافية اعترضوا على ذلك، بل إن الخطة ولدت معارضة شعبية دفعت الآلاف إلى النـزول إلى الشوارع في أكثر من ثلاثين مدينة في أنحاء البلاد احتجاجاً على التغييرات المقترحة.

وبعد تعرضها لضغوطات، تراجعت الحكومة عن خطتها؛ مبقية في النهاية فلترين فقط للمحتويات: مستوى ، ومستوى ، يمكن للمستخدم اختيار

أحدهما وفق رغبته. لكن الجدل لم ينته هنا، فقد أفادت مجموعات حريات الإعلام بأن الاختبارات التي أجرتها على نظام الرقابة كشفت عن وجود إطار فلترة أكثر تشدداً مما أقرت به الهيئة. فإضافة إلى المصطلحات المتوقع حجبها، والمتعلقة بالمحتويات الإباحية أو العنيفة، وجدت المجموعات أن مواقع أخبار عادية، ومحتويات متحررة ثقافياً أو غربية، وكلمات مفتاحية مرتبطة بالأقلية الكردية، كانت جميعها محجوبة ضمن النظام الجديد. ويقول بعض الناشطين إن حجب معلومات عن المنظمات الانفصالية الكردية تحت فلتر مستوى دليل على سوء نية الدولة؛ وقد أطلقت مجموعة مراقبة وسائل الإعلام العالمية، ، على السياسة التركية تسمية "الرقابة من الباب الخلفي".

واستجابت الحكومة التركية لبعض المخاوف الشعبية حيال النظام الجديد. لكن الشفافية المتوفرة حول المحتويات الخاضعة للرقابة ضمن هذه السياسات ضئيلة، إن وجدت، لذا لا يبقى على الحكومة سوى أن تنتظر لحظة الرد عندما تبدأ تذمرات كهذه بالظهور بين المواطنين. فالنموذج الخجول لفلترة الإنترنت يجمع بين قدرة الحكومة على تفادي المحاسبة وبين استعدادها لاتخاذ إجراءات بناءة عندما تتصاعد الضغوطات. وهو أسلوب مغرٍ بالنسبة إلى البلدان ذات المجتمعات المدنية النامية التي تكون المؤسسات الحكومية فيها قوية أيضاً. أو بالنسبة إلى الحكومات التي لا تتمتع بقواعد دعم يعتمد عليها، لكنها تجمع بين يديها ما يكفي من السلطة لاتخاذ قرارات من جانب واحد كهذه.

أما الأسلوب الثالث للفلترة، وهو الأسلوب المقبول سياسياً وثقافياً، فتتنوع الدول التي تطبقه، من كوريا الجنوبية إلى ألمانيا وماليزيا. وهو ينحصر بالفلترة الانتقائية المحدودة لمحتويات بعينها بناءً على أسس قانونية، من دون محاولة إخفاء الرقابة أو دوافعها. وقد يتذمر بعض الناشزين من بين السكان، لكن غالبية المواطنين تتفق في معظم الأحيان مع سياسات الفلترة لأسباب تتعلق بالأمن والصالح العام. ففي كوريا الجنوبية على سبيل المثال، يجرّم قانون الأمن القومي صراحةً التعبير العلني عن الدعم لكوريا الشمالية في الفضاءين المادي والافتراضي. وتعمل حكومة كوريا الجنوبية على فلترة محتوى الإنترنت بانتظام من المحتويات العائدة لجارتها الشمالية. وفي عام 2010 أُفيد عن حجب الحكومة حوالى أربعين موقع وب مرتبطاً بالنظام الكوري الشمالي أو داعماً له، وإغلاقها مجموعةً من الحسابات التي يحتمل أن تكون على صلة ببيونغ يانغ على مواقع الشبكات الاجتماعية، كالفيسبوك وتويتر، وإجبارها مديري المواقع على حذف أكثر من أربعين ألف مدخلة مدونة مناصرة لكوريا الشمالية.

وفي ألمانيا قوانين قوية لمكافحة خطاب الكراهية تعتبر إنكار الهولوكوست والخطاب النازي الجديد خروجاً على القانون. لذلك تعمل الحكومة على حجب مواقع الوب التي تعبر عن مثل هذه المواقف في ألمانيا. وفي ماليزيا، وعلى الرغم من قطعها الوعود لمواطنيها بعدم تطبيق أية رقابة على الإنترنت (وصل بها الأمر إلى تشريع ذلك في قانون الضمانات)، تم فجأةً حجب الوصول إلى مواقع لمشاركة الملفات - مثل ميغا.أبلود وبايريت.باي - عام 2011 بحجّة أن هذه المواقع تنتهك

قانوناً آخر هو قانون حقوق الملكية الفكرية للبلاد العائد لعام 1987. ودافعت لجنة الاتصالات والوسائط المتعددة الماليزية في بيانٍ لها عن هذه الخطوة قائلة إن "الامتثال للقوانين يجب ألا يفسر على أنه رقابة"، وهو ما يختلف معه الكثير من الماليزيين، لكن الحجب يبقى مقبولاً سياسياً وقانونياً.

من بين هذه النماذج الثلاثة، سيتمنى الناشطون أن يكون النموذج الثالث هو المعيار السائد بين الدول في العالم، لكن ذلك يبدو مستبعداً. فالبلدان ذات الشعوب الناشطة والمطلعة هي وحدها المضطرة لأن تكون بهذه الشفافية والتقيد، وبما أن معظم الحكومات ستتخذ مثل هذه القرارات قبل أن يصبح مواطنوها على اتصال تام، فلن يكون لديها دافعٌ كبير للترويج على نحوٍ فعال لهذا النوع من الإنترنت الحرة والمنفتحة الذي نراه في بلدان "النموذج المقبول سياسياً".

ستحافظ النـزعات التي نشهدها اليوم على اتجاهاتها بطرقٍ يمكن توقع معظمها على نحوٍ معقول. إذ ستشعر الحكومات بأنها تخوض معركةً خاسرةٍ ضد الإنترنت التي لا تنفك تتغير وتستنسخ محتوياتها. وسيزداد دور البلقنة نظراً إلى كونها آليّة مفضلة لمواجهة هذا التحدي، وستكون المرحلة التالية في هذه العملية بالنسبة للكثير من الدول هي التحرير التعاوني، حيث ستقوم الدولة بتشكيل مجموعات ذات مصلحة لتتعاون معاً على تحرير الوب؛ بناءً على سياسات جغرافية أو قيم مشتركة. وسيكون الحراك التعاوني (سواء أكان في العالم المادي أم الافتراضي) حركةً منطقية بالنسبة لكثيرٍ من الدول التي تعوزها الموارد أو تعجز عن الوصول إلى مناطق واسعة أو السيطرة عليها. وحتى مع البلقنة، سيبقى الفضاء السايبري ميداناً أوسع من أن تتم تغطيته. فتماماً كما تزيد بعض الدول الموارد العسكرية لدولٍ أخرى لضمان أمن قدرٍ أكبر من الأرض الفيزيائية، كذلك ستشكل الدول تحالفاتٍ للتحكم بمزيد من المساحات الافتراضية، وستجد الدول الكبرى في التعاون شرعنةً لمحاولات الفلترة التي تقوم بها، وتحويلاً لأنظارٍ غير مرغوبٍ فيها (العذر القائل "انظر، هناك آخرون يقومون بذلك أيضاً"). وستجد الدول الصغرى في التحالفات ضمن هذه الخطوط طريقةً رخيصةً للتقرب من اللاعبين الكبار ولتحقيق مكاسب من المهارات التقنية المفيدة والسعات التي قد تحتاج إليها في أوطانها بالوقت نفسه.

قد يبدأ التحرير التعاوني مع بعض الاتفاقيات الثقافية البسيطة أو العداوات المشتركة بين الدول؛ فينتج على سبيل المثال عن وجود أقليات دينية لا تحبها هذه الدول، أو عن نظرتها إلى أجزاء أخرى من العالم أو موقفها الثقافي من شخصياتٍ تاريخية مثل فلاديمير لينين، وماوتسي تونغ، ومصطفى كمال أتاتورك. وفي العالم الافتراضي، ستشكل الحساسيات الثقافية أو العرقية المشتركة قوة تجاذبٍ بين الدول؛ بما فيها دولٌ ربما ما كانت لتتقارب لولا هذه الحساسيات. وسيكون احتمال مشاركة الدول الكبرى في ذلك أقل من احتمال مشاركة الصغيرة منها (فهي تتمتع مسبقاً بالقدرات التقنية). أي إننا سنكون أمام أسطولٍ من دول أصغر حجماً تستجمع مواردها معاً، وتجد هذه الطريقة مفيدة. فإذا طفح كيل إحدى الدول

الأعضاء في رابطة الدول المستقلة - وهي اتحادٌ يجمع دول الاتحاد السوفييتي السابق - من إصرار موسكو على توحيد اللغة الروسية في المنطقة، يمكنها التعاون على تطبيق الرقابة على المحتويات ذات اللغة الروسية كلها في شبكات الإنترنت الوطنية لديها لتحدّ بالتالي بالكامل من وصول روسيا إلى مواطنيها.

من المرجح أن تكون الإيديولوجيا والأخلاقيات الدينية هي المحرك الأقوى لمثل هذه التعاونات؛ وهي تمثل منذ اليوم أقوى دوافع الرقابة. فتخيل ما سيحدث لو شكلت مجموعةٌ من الدول المحافظة جداً تحالفاً شبكياً يقوم على قيمها المشتركة وحاجاتها الاستراتيجية، وقررت أن تبني "شبكة وب تنسجم مع قيمها". مع أن شبكة الوب هذه ستكون جزءاً من الإنترنت الكبرى على أية حال، إلاّ أنها ستصبح المصدر الرئيس للمعلومات والأخبار والتاريخ والنشاط بالنسبة للمواطنين المقيمين في هذه البلدان. وإذا كان تطور الإنترنت وانتشارها قد تحدّدا على مدى سنواتٍ إلى حدٍّ بعيد بالمعيار الذي يتخذ الإنكليزية لغةً وحيدة له، فإن التحقيق المستمر لأسماء النطاق الدولية التي تسمح باستخدام أسماء نطاقات مكتوبة بأحرف غير رومانية والوصول إليها (مثل http://اختبار.مثال) سيغير هذا الواقع. وسيكون إنشاء شبكة الوب، بل وأي إنترنت مؤممة، أكثر إمكانيةً إذا استطاع مستخدموها الوصول إلى نسخة من الإنترنت مكتوبة بلغتهم وأبجديتهم.

ويمكن للإنترنت ضمن شبكة الوب، وفقاً لهوية من يشارك فيها أو يقود عملية تطويرها، أن تكون محابيةً للشريعة، فتبدو فيها التجارة الإلكترونية والصيرفة الإلكترونية مختلفةً؛ حيث لا يسمح فيها لأحدٍ بأخذ فائدة. وقد تراقب الشرطة الدينية الأحاديث التي تجري على الشبكة، وتتعاون مع القوى التنفيذية المحلية للإبلاغ عن الخروقات. وربما تجد الأقليات الإثنية والدينية نفسها خاضعةً لرقابةٍ مشددة أو قيودٍ صارمة، أو حتى إلى الإقصاء. ستختلف ضمن هذا السيناريو إمكانية التفاف مواطنٍ محلي عارف بالتقانة على هذه الإنترنت للوصول إلى شبكة الوب العالمية وفقاً للبلد الذي يعيش فيه. فربما لا تكون موريتانيا راغبةً أو قادرةً على إيقافه، أما الدول الأكثر تطوراً وقدرة فستكون قادرة على ذلك على الأرجح. من جهةٍ أخرى، إذا شعرت الحكومة الموريتانية بالقلق من تجاوز مستخدميها شبكة الوب الحديثة، فلا شك في أن أحد شركائها الرقميين الجدد سيتمكن من مساعدتها على إعلاء السياج. وضمن إطار تحالفات التحرير التعاوني، ستسمح الدول الأقل ارتياباً لشعوبها بالوصول إلى كلتا النسختين من الإنترنت (في ما يشبه التحكم الأسري الاختياري في التلفاز)؛ مراهنةً على تطبيق المستخدمين للمحتويات الأكثر أماناً والمفصلة على نحوٍ خاص، بدلاً من أن تعتمد على القوة وحدها.

ستظهر حالات تقوم فيها الدول الديمقراطية والاستبدادية بالاشتراك في تحرير محتويات الوب. ويحدث مثل هذا التعاون عادة عندما تكون لديمقراطية ضعيفة جارة مستبدة أقوى تجبرها على القبول بتنازلات في العالم الرقمي؛ على غرار تلك التي تقوم بها في العالم الحقيقي. وستكون هذه إحدى الحالات النادرة التي يلعب فيها القرب المادي دوراً مؤثراً في الشؤون الافتراضية. فمنغوليا على سبيل المثال ديمقراطية فتية لديها إنترنت منفتحة، لكنها محصورة بين روسيا والصين، وهما

بلدان كبيران، لكل منهما سياساته الخاصة في تقييد الإنترنت. وقد شرح لنا رئيس الوزراء المنغولي السابق، سوخباتار باتبولد، كيف أنه يرغب لمنغوليا - مثلها مثل أي بلد آخر - بأن تتمتع بهويتها الخاصة؛ بمعنى - على حد قوله - أن تكون لها علاقات جيدة مع جيرانها تمنعهم من التدخل في شؤونها. "إننا نحترم حق كل بلد في سلوك طريقه الخاص في التنمية"، يقول، "ونحن ندرك المسافة التي يجب أن ننأى بها بأنفسنا عن مواضيع تيبيت وتايوان اللتين لا تتدخلان في شؤوننا. وهذا ما ينطبق أيضاً على روسيا التي يربطنا بها عهد طويل من العلاقات".

من الأسهل في العالم المادي الحفاظ على موقف حيادي يقوم على عدم التدخل. أمّا العالم الافتراضي فيعقّد هذا النموذج إلى حد بعيد لأن الناس هم الذين يحكمون النشاطات على الشبكة. والناس المتعاطفون مع المجموعات المعارضة والأقليات الإثنية في الصين وروسيا سيجدون في منغوليا مكاناً مثالياً للتجمع. فقد يلجأ أنصار متمردي أويغور أو تيبيت أو الشيشان إلى استخدام فضاء الإنترنت المنغولي كقاعدة للتعبئة وشن الحملات الشبكية وبناء الحركات الافتراضية. وعندها، ستجد الحكومة المنغولية نفسها بلا شك عرضة لضغوطات صينية وروسية، وليس على الصعيد الدبلوماسي فقط؛ فبنيتها التحتية الوطنية ليست مصممة للصمود في وجه هجوم سايبري من أي من الجارتين. وسعياً لإرضاء جارتيها والحفاظ على سيادتها المادية والافتراضية، قد تجد منغوليا أنّه من الضروري الانصياع إلى الإملاءات الصينية أو الروسية، وفلترة محتويات الإنترنت المرتبطة بالمواضيع الإشكالية. وسيكون الخاسرون من هذا التنازل هم المنغوليون الذين ستسرق منهم حريتهم الشبكية بسبب قوى أجنبية أنانية مشاكسة.

لن تسعى جميع الدول إلى التعاون مع غيرها خلال عملية البلقنة، لكن النتيجة النهائية ستكون نفسها؛ خليطاً من المصالح الوطنية والحدود الافتراضية. فالتوجه نحو منصات معولمة مثل الفيسبوك وغوغل يولّد نظاماً للتقانة أكثر قابليةً للانتشار؛ مما يعني توزيعاً على نطاقٍ أوسع لأدوات الهندسة التي تسمح للناس باستخدامها لبناء بناهم الشبكية الخاصة. ومن دون تشريعات من الدولة تكبت الابتكار، سيندزع هذا النمو إلى التسارع تسارعاً كبيراً. فخلال المراحل الأولى، لن يدرك المستخدمون أنهم قد أصبحوا على إنترنت تخص بلداً آخر نتيجة شفافية هذه التجربة كما هي اليوم، لكن مع انكباب الدول على شقّ طريقها نحو الاستقلالية في العالم الافتراضي، سيشعر معظم المستخدمين بتغيرٍ بسيطٍ جداً.

لكن هذا الاستتباب لن يطول، وما بدأ على شكل وب عالمية سيبدأ باتخاذ مظهرٍ أكثر شبهاً بالعالم نفسه؛ أي إنه سيعجّ بالانقسامات الداخلية والمصالح المتضاربة. وسيظهر شكلٌ ما من تأشيرة الدخول على الإنترنت، تكون سريعة وإلكترونية، كوسيلةٍ لاحتواء دفق المعلومات في كلا الاتجاهين، حيث يُطلب من المستخدمين التسجيل والموافقة على شروطٍ معينة للوصول إلى الإنترنت الخاصة بالبلد. فإذا قررت الصين أنه يتوجب على جميع الخارجيين أن تكون بحوزتهم فيزا للوصول إلى الإنترنت الصينية، فسيكون لذلك أثرٌ بالغٌ على مشاركة المواطنين وعلى العمليات التجارية الدولية والتقارير الاستقصائية. وهو ما يذكّر - إلى جانب القيود الداخلية

المفروضة على الإنترنت - بمكافئ القرن الحادي والعشرين للساكوكو (البلد المقفل) الياباني الشهير، وهو سياسةُ عزلٍ شبه تام تمّ تبنيها في القرن السابع عشر.

قد تطبق بعض الدول شروط تأشيرة الدخول كأداةٍ لمراقبة الزوار الدوليين، وكإجراء مدر للدخل في الوقت نفسه. حيث ستُفرض رسومٌ بسيطة آلياً عند دخول الفضاء الافتراضي للبلاد، بينما تفرض رسومٌ أعلى إذا انتهك الشخص خلال نشاطاته الشبكية (التي ستتتبعها الحكومة بواسطة الكوكيز وأدواتٍ أخرى) شروط الفيزا. وستظهر تأشيرات الدخول الافتراضية كاستجابةٍ لتهديداتٍ أمنية متعلقة بهجوماتٍ سايبرية. فإذا كان عنوانك على الإنترنت قادماً من بلدٍ مدرجٍ على اللائحة السوداء، فإنك ستواجه حواجز أعلى، ومراقبةً أشد.

إلا أن دولاً أخرى ستلجأ إلى الاستعراض أمام العالم، وستحجم عن تطبيق التأشيرات لإظهار التزامها بمبدأ البيانات المفتوحة، ولتشجيع دولٍ أخرى على أن تحذو حذوها. ففي عام 2010 أصبحت تشيلي أول بلدٍ في العالم يصادق على قانونٍ يضمن حيادية الشبكة وصرّحت بذلك. ومع وجود حوالى نصف سكان تشيلي البالغ عددهم 17 مليوناً على الشبكة، ومع استمرار البلاد في تطوير بنيتها التحتية التقانية، لا شك في أن تصريحات علنية كهذه ستحبب تشيلي لدى حكومات أخرى تساندها في سياساتها الاستشرافية في مجال الاتصالات. وستفضل البلدان الواقفة على عتبة الإنترنت النموذج التشيلي على غيره. فقد يطلب منها التوقيع مع بلدان أخرى، تريد بناء علاقات تجارية تعتمد على منصات تجارة إلكترونية أو منصات مشابهة معها، على تعهدات بعدم إلزام المستخدمين بتأشيرة الدخول، في ما يشبه تطبيق اتفاقية شينغين (المنطقة الخالية من الحدود في أوروبا) في العالم الافتراضي.

ضمن شروط كهذه، سيشهد العالم أول طلب لجوء على الإنترنت. فالمعارض الذي لا يستطيع أن يعيش بحرية مع إنترنت استبدادية، ولا يُسمح له بولوج شبكات إنترنت تعود إلى بلدان أخرى، سيسعى للحصول على لجوء مادي في بلد آخر للوصول إلى الحرية الافتراضية على الإنترنت الخاصة بهذا البلد. وقد يكون ثمة شكل من أشكال اللجوء الافتراضي المؤقت، حيث يقدم البلد المضيف خدمة بروكسي متطورة وأدوات التفاف تسمح للمعارض بالاتصال بالخارج. وقد يكون الحصول على اللجوء الافتراضي خطوة أولى هامة على طريق الوصول إلى اللجوء المادي، فهي إشارة إلى الثقة من دون الالتزام الكامل. وسيمثل اللجوء الافتراضي في هذه الحالة طبقة حماية إضافية ريثما تصل قضية اللجوء المادي إلى المحاكم.

لكن اللجوء الافتراضي لن يكتب له النجاح إذا حدث التصعيد الأخير المتمثل بنظام أسماء نطاق بديل (دي.إن.إس)، أو حتى بالتأثير على النظام القائم تأثيراً عنيفاً وشاملاً حيث يتم تقديم مصالح الدولة. فالإنترنت كما نعرفها اليوم تستخدم نظام أسماء النطاق لمقابلة الحواسب والأجهزة مع موارد البيانات الموافقة، وذلك بترجمة عناوين الإنترنت (وهي عبارة عن أرقام) إلى أسماء قابلة للقراءة وبالعكس. وتقوم متانة الإنترنت على اعتماد جميع الحواسب والشبكات للجذر الرسمي لنظام أسماء النطاق (الذي تقوم على تشغيله هيئة الإنترنت للأسماء

والأرقام المخصصة، أو إيكان)، والذي يحتوي على جميع نطاقات القمة التي تظهر في لاحقات عناوين الوب (edu, .com, .net وغيرها).

إلا أنه ثمة جذور بديلة لنظام نطاق الأسماء (وهي موجودة على التوازي مع الإنترنت من دون أن تكون مرتبطة بها). وثمة اعتقاد سائد في الدوائر التقنية بأن ابتكار نظام أسماء نطاق بديل يعارض كل ما تمثله الإنترنت وما بنيت لتحقيقه؛ أي التبادل الحر للمعلومات. وصحيح أن أية حكومة لم تتمكن حتى الآن من التوصل إلى نظام بديل*، إلا أنها إذا نجحت في تحقيق ذلك بالفعل فستتمكن من فصل شعبها فعلاً عن الإنترنت العالمية لتستبدلها بمجرد شبكة إنترانيت وطنية مغلقة؛ الأمر الذي يستلزم من الناحية التقنية إنشاء بوابة خاصّة للرقابة بين البلد وبقية العالم، مع الاستعانة بوكيل (بروكسي) بشري يسهل عمليات نقل البيانات الخارجية عندما يكون ذلك ضروريًّا؛ كما في الحالات المتعلقة بموارد الدولة على سبيل المثال.

أما بالنسبة إلى الشعب، فستصبح إجراءات البروكسي الشائعة - كالشبكات الخاصة الافتراضية ونظام تور - بلا معنى، لأنه لن يكون هناك ما يتم الاتصال به. إنها النسخة الأكثر تطرفاً مما يسميه مختصو التقانة "الحديقة المسورة". وتعني الحديقة المسورة في مجال الإنترنت بيئة التصفح التي تتحكم بوصول المستخدم إلى المعلومات والخدمات على الشبكة (وهو مفهوم لا ينحصر بالمناقشات الدائرة حول الرقابة، بل له جذور أعمق امتداداً في تاريخ تقانة الإنترنت. فقد سبق لكل من إيي.أو.إل وكومبوسيرف، عملاقتي الإنترنت في ذلك الوقت، أن أطلقتا حدائق مسورة). ولكي يحقق الفصل مفعوله الكامل، ستطلب الحكومة من الموجهات الإحجام عن الإعلام عن عناوين الإنترنت لمواقع الوب (خلافاً لأسماء النطاق، ترتبط عناوين الإنترنت بالمواقع نفسها ارتباطاً ثابتاً)؛ مما سيؤدي إلى عزل هذه المواقع على جزيرة نائية جداً، ويجعل الوصول إليها مستحيلاً عملياً. وأياً كان المحتوى الموجود على الشبكة الوطنية، فسيتم تدويره داخلياً ليبقى عالقاً وكأنه عنقود من الفقاعات في شاشة توقف على الحاسب. وستصطدم أية محاولات للوصول إلى المستخدمين على هذه الشبكة من الخارج بسد منيع. وهكذا يصبح من الممكن بنقرة واحدة على جهاز توزيع الشبكة إخفاء بلد كامل من على الإنترنت.

ليس هذا جنوناً كما يبدو للوهلة الأولى. فقد جاءت أولى التقارير عن وجود خطة قيد التنفيذ لدى الحكومة الإيرانية لبناء "إنترنت حلال" عام 2011. وبعد مرور أكثر من عام، كان يبدو أن الافتتاح الرسمي قد بات وشيكاً. وأطلق النظام في كانون الأول من عام 2012 موقع مهر، وهو نسخته الخاصة من يوتيوب، مع "فيديوهات مصادق عليها من الحكومة"، ليكون مؤشراً إضافياً على جدية النظام في مشروعه. وبقي الغموض يلف تفاصيل الخطة، لكن وفقاً للمسؤولين في الحكومة الإيرانية، ستتاح للإيرانيين إنترنت وطنية "نظيفة" كرديف للإنترنت العالمية (المثقلة بالرقابة بدورها)، لكنها ستحل يوماً ما محل الإنترنت برمتها، وهو ما يتطلب نقل جميع المواقع "الحلال" إلى مجال معين من عناوين الإنترنت حيث تصبح فلترة المواقع الواقعة خارج كتلة الحلال أمراً هيناً، ثم تقوم الحكومة مع المؤسسات التابعة لها

بتأمين المحتويات لشبكة الإنترانيت الوطنية، سواء أفعلت ذلك بجمعها من شبكة الوب العالمية وتنظيفها، أو بوضع هذا المحتوى يدوياً. وعندها ستتم مراقبة جميع النشاطات على الإنترنت عن كثب بفضل السيطرة والسلطة اللتين تتمتع بهما الحكومة - عبر بنيتها التحتية عالية المستوى - على البرمجيات (وهذا أمر يوليه المسؤولون الإيرانيون اهتماماً شديداً؛ كما يبين الحظر الذي فُرض عام 2012 على استيراد برمجيات الأمن الحاسوبـي الأجنبية). وقد أخبر وزير الشؤون الاقتصادية الإيراني وكالة الأنباء الحكومية في البلاد أنهم يأملون أن تحل محل الوب في البلدان المسلمة الأخرى أيضاً، على الأقل في تلك التي يعيش فيها ناطقون بالفارسية.

قد يكون التهديد الإيراني مجرد خدعة. فليس من الواضح بعد كيف تنوي الدولة تماماً أن تمضي في مشروعها، من الناحيتين التقنية والسياسية على حدٍّ سواء، وكيف ستتجنب سخط تلك الشريحة العريضة جداً من شعبها القادرة على الوصول إلى الإنترنت. إذ يعتقد البعض أنه سيستحيل فصل إيران عن شبكة الإنترنت العالمية كليًّا؛ بسبب اعتمادها الاقتصادي الكبير على ارتباطاتها الخارجية. بينما يخمن آخرون أن إيران، إذا لم تستطع بناء نظام أسماء بديل، فقد تدشن نموذج إنترنت مزدوجة سترغب الدول القمعية الأخرى في اتباعه أيضاً. وأيا كانت الطريق التي ستختارها إيران، وإذا نجحت في مساعيها، فستتفوق "الإنترنت الحلال" على جدار الصين الناري العظيم لتصبح بجدارة الحالة الأكثر تطرفاً للرقابة على المعلومات في التاريخ. ومن شأنها أن تغير شكل الإنترنت الذي نعرفه اليوم.

تعددية الأطراف في العالم الافتراضي

على التوازي مع محاولات البلقنة هذه، سنشهد تصاعداً في التحالفات متعددة الأطراف في العالم الافتراضي، حيث ستتشكل بناءً على التضامن الإيديولوجي أو السياسي، وتشارك فيها الدول والشركات على حدٍّ سواء لتعمل معاً ضمن تحالفاتٍ رسمية. فدول مثل بيلاروسيا وأريتريا وزيمبابوي وكوريا الشمالية (وهي دولٌ مستبدة مع ثقافة عبادة فرد قوية في حين نجدها منبوذةً في الأماكن الأخرى من العالم)، لن يكون لديها شيءٌ تخسره إذا انضمت إلى اتحادٍ سايبري مستبد يمكن فيه تشارك تقانات الرقابة والمراقبة واستراتيجياتهما. ومع تعاون هذه البلدان على بناء دولٍ بوليسية في العصر الافتراضي، ستزداد صعوبة إدارة الشركات الغربية للأعمال من وجهة نظر العلاقات العامة في تلك الأماكن؛ حتى إذا كان ذلك قانونياً. بينما سينشأ فضاء مؤاتٍ لشركات غير غربية يعاني مساهموها قدراً أقل من تأنيب الضمير، وتكون معتادةً على العمل في بيئاتٍ مشابهة؛ حيث تلعب دوراً تجارياً أكثر فعالية ضمن شبكةٍ من الدول المستبدة.

فليس من المصادفة في شيء على سبيل المثال أن تكون الشركة التي تمتلك 7 بالمئة من شبكة الهواتف النقالة الرسمية الوحيدة في كوريا الشمالية، كوريولينك، هي شركة الاتصالات المصرية أوراسكو التي ازدهرت تحت حكم حسني مبارك الطويل (وتعود النسبة المتبقية والبالغة 25 بالمئة إلى وزارة البريد والاتصالات

الكورية الشمالية). أما المشتركون الكوريون الشماليون، فتمثل خدمة كوريو لينك بالنسبة إليهم حديقةً مسورة؛ فهي منصة في غاية المحدودية، لا تسمح سوى بالوظائف الأساسية. ولا يمكن لمستخدمي كوريولينك إجراء الاتصالات الدولية أو استقبالها، كما لا يمكنهم الوصول إلى الإنترنت (يمكن للبعض في كوريا الشمالية الوصول إلى شبكة الإنترانت الكورية الشمالية، والتي ليست سوى خليط من المحتويات الافتراضية، الدعائية في معظمها، التي قام مسؤولو الحكومة بنقلها من الإنترنت). وتتم مراقبة مكالمات الهاتف المحلية والرسائل النصية بشكلٍ دائمٍ تقريباً. فقد أفادت مجلة الإيكونوميست أن هذه الشبكة تمثل بالفعل منصةً لنشر الدعاية الحكومية، حيث تقوم خدمة رودونغ زنمون (جريدة العمال) بإرسال آخر الأخبار إلى المستخدمين كرسائل نصية، ويتم "تشجيع" الناس على دفع فواتير هواتفهم باليورو (الذي يتم تدويره بشكلٍ غير رسمي)، وإن كان ذلك غير ملزم؛ وهي مهمةٌ صعبة بالنسبة لمعظم الكوريين الشماليين. وعلى الرغم من كل ذلك، كان الطلب على الهواتف مرتفعاً إلى درجة أنها اجتاحت البلاد عندما ارتفع عدد المشتركين من ثلاثمئة ألف إلى أكثر من مليون خلال فترةٍ لا تتجاوز ثمانية عشر شهراً حتى بداية عام 2012. ويبقى هامش الربح التشغيلي الإجمالي لكوريولينك، والبالغ 80 بالمئة، عملاً رابحاً بالنسبة لأوراسكوم.

وفي إيران، بعد القمع العلني جداً للحركة الخضراء في البلاد عام 2009، عمدت شركات التقانة الغربية، مثل إيريكسون ونوكيا وشبكات سيمينس نوكيا، إلى النأي بنفسها عن النظام. وفي غيابها، ظهرت عملاقة الاتصالات الصينية هاواوي، واغتنمت الفرصة لتسيطر على سوق الهاتف النقال الإيرانية الضخمة (التي تسيطر عليها الدولة). وبينما كانت سابقاتها من الشركات الغربية تعاني من ردود فعلٍ سلبية في بلدانها نتيجةً لبيعها الحكومة الإيرانية منتجاتٍ يتم استخدامها في تعقب الناشطين الديموقراطيين وقمعهم، عملت هاواوي على الترويج لمنتجاتها بنفحةٍ محابيةٍ للاستبداد. فقد جاءت قائمة منتجاتها - وفقاً لقصةٍ من مجلة وول ستريت - من غير حياء، حيث اشتملت على منتجاتٍ مثل "تجهيزات تعقب بناءً على الموقع" للسلطة التنفيذية (والتي تم شراؤها مؤخراً من قبل أكبر مشغل هواتف خلوية في إيران)، وخدمة أخبار نقالة مساعدة على الرقابة. وتعتبر شركة زعيم للاتصالات الإلكترونية، الشريك المحلي المفضل لهاواوي؛ الشريك المفضل للفروع الحكومية أيضاً، بما فيها الحرس الثوري ومكتب الرئاسة.

وتزعم هاواوي رسمياً أنها تقدم لشركة زعيم "خدمات ومنتجات تجارية للاستخدام العام" فقط، إلا أنه وفقاً لمجلة وول ستريت، ومن خلال اجتماعات غير رسمية مع مسؤولين إيرانيين، فإن هاواوي لم تترك مجالاً للشك في خبرتها في مجال رقابة المعلومات التي صقلتها في الصين (سارعت هاواوي إلى نشر بيان صحفي بعيد نشر القصة أنكرت فيه العديد من هذه الادعاءات، وصرحت بعد ذلك بشهر بأنها "ستحدّ طوعياً" من عملياتها التجارية نتيجة "ازدياد تعقيد الوضع").

ورداً على هذه التحالفات بين البلدان المستبدة، ستسعى الدول الديموقراطية بدورها إلى بناء تحالفاتٍ مشابهة وشراكاتٍ عامة - خاصة للترويج لإنترنت أكثر

انفتاحاً توفر قدراً أعظم من الحرية السياسية والاقتصادية والاجتماعية. وسيكون أحد الأهداف هو احتواء المراقبة وتقنياتها والفلترة الصارمة جداً في البلدان ذات الانتشار المنخفض، لكن النامي، للإنترنت. وقد يتجلى ذلك في الكثير من الاستراتيجيات المختلفة، منها حزَم المساعدة الثنائية مع شروط مسبقة محددة. وجُعِل انفتاح الإنترنت هدفاً سياسياً رئيساً لسفراء البلاد. فقد يتم شن حملات عابرة للحدود الوطنية لتغيير الإطار القانوني الدولي في ما يتعلق بحرية التعبير والبرمجيات مفتوحة المصدر. إذ ستطغى أهداف "الصورة الكبيرة" المشتركة لهذه الدول (الوصول إلى المعلومات وحرية التعبير والشفافية)، على السياسات الصغرى أو الفروق الثقافية في ما بينها، مولّدةً نوعاً من الرابطة الهانـزية التي تُبعث إلى الحياة في مجال الاتصالات. أمّا الرابطة الهانـزية فهي رابطة كانت تسوس السلطة الجمعية عبر أوروبا الشمالية بين القرنين الثالث عشر والخامس عشر عبر تحالفاتها الاقتصادية بين مدن - دول متجاورة. ويمكن أن يكون مكافئها المعاصر مبنياً على مبادئ مشابهة من المساعدة المتبادلة، لكن ضمن نسخةٍ معولمة أكبر. ولن تعتمد التحالفات إلى ذلك الحد على الجغرافيا بعد الآن، فالمسافة واحدة في الفضاء الافتراضي بين جميع الأشياء، وإذا كانت دولتا الأورغواي وبنين تجدان سبباً ما للعمل معاً، فإن تنفيذ ذلك اليوم أسهل منه في أي وقتٍ مضى.

سيتطلب الدفاع عن حرية المعلومات والتعبير في جزء منه عنصراً جديداً من المساعدة العسكرية. إذ سيشتمل التدريب على المساعدة التقنية ودعم البنية التحتية؛ بدلاً من الدبابات والغاز المسيل للدموع، ولو أن الأخير سيبقى على الأرجح جزءاً من الاتفاقيات. فما كانت شركة لوكهيد مارتين تمثله في القرن العشرين ستجسده شركات الأمن السايبري والتقاني في القرن الحادي والعشرين. فالشركات العاملة في صناعة الدفاع التقليدية، مثل نورثروب غرومان وريثون، تتعاون منذ اليوم مع الحكومة الأمريكية لتطوير سعة سايبرية. وإذا كانت شركات صناعة الأسلحة وبناء الطائرات وغيرها من عناصر المشهد الصناعي العسكري لن تنحسر (فالجيوش التقليدية ستحتاج دائماً إلى البنادق والدبابات والحوامات)، فإن العمليات العسكرية الكبرى، والتي تم تخصيصها إلى حد بعيد، ستقتطع من ميزانيتها جزءاً تخصصه للمساعدة التقنية.

ستكتسب المساعدة الخارجية والدعم التنموي بعداً رقمياً أيضاً؛ مرتكزين على هذه التحالفات الجديدة متعددة الأطراف. ومقايضة المساعدة الخارجية بالنفوذ المستقبلي ستبقى كما هي، لكن المكونات التي ستشتمل عليها ستتغير. ففي بلدٍ نامٍ معين، قد تقوم قوةٌ أجنبيةٌ ما بمدّ الطرقات، بينما تستثمر أخرى في مجال الزراعة، وتقوم ثالثة ببناء الشبكات والأبراج الخلوية. ففي العصر الرقمي تصبح التقانة الحديثة أداةً جديدةً لصياغة التحالفات مع الدول النامية، وعلينا ألا نقلّل من أهمية الكفاءة التقانية بالنسبة لهذه البلدان وحكوماتها. فقد يأتي الضغط من أجل المساعدة الخارجية؛ متجسدة على شكل شبكات سريعة وأجهزة حديثة وعرض حزمة رخيص ووفير، من قبل الشعب الذي سيضغط على الحكومات للموافقة على

الشروط المسبقة الأساسية. وأياً كان دافعها، ستضع دول المستقبل في العالم النامي رهاناً طويل الأمد على الاتصالات، وسترتب علاقاتها الدبلوماسية وفقاً لها.

ستتشكل تحالفاتٌ جديدة بناءً على المصالح التجارية أيضاً، وخصوصاً في ما يتعلق بمواضيع حقوق الملكية الفكرية. فمع تقدم التجارة المضطرد في العالم الافتراضي، ستؤدي الديناميات المتعلقة بتطبيق الحقوق الفكرية إلى ظهور طبقة أخرى من التحالفات والعداوات الافتراضية. فلا تزال معظم قوانين حقوق الملكية الفكرية متركزةً على فكرة البضائع المادية، وما زالت المواقف تختلف إزاء اعتبار السرقة والقرصنة للبضائع الافتراضية (الأفلام والموسيقا وغيرها من المحتويات) معادلةً لسرقة النسخ الفيزيائية من هذه السلع. لكن الدول ستبدأ في المستقبل بخوض معارك أعمق حول حقوق الملكية الفكرية وحقوق الطبع والنشر لأن صحة قطاعاتها التجارية ستكون على المحك.

أُبرمت العديد من الاتفاقيات الدولية التي تعالج قوانين حقوق الملكية الفكرية كميثاق بيرن عام 1886 الذي يتطلب الاعتراف المتبادل بالحقوق الفكرية مع الدول الموقعة الأخرى، واتفاقية شؤون حقوق الملكية الفكرية المتعلقة بالتجارة لعام 19 التي تعين الحد الأدنى من معايير حقوق الملكية الفكرية في دول منظمة التجارة العالمية، واتفاقية حقوق النشر التي أبرمتها منظمة حقوق الملكية الفكرية العالمية عام 1996، والتي تحمي الحقوق الفكرية لتقانة المعلومات من الاختراق. وتحكم هذه القوانين حقوق النشر حول العالم بالطريقة نفسها بشكلٍ عام، لكن كل بلدٍ مسؤولٌ عن تنفيذها ضمن حدوده. وتختلف البلدان في مدى يقظتها، فنظراً لسهولة انتقال المعلومات عبر الحدود فإن مقرصني المواد ذات الحقوق الفكرية يجدون عادةً ملاذاً افتراضياً آمناً في البلدان ذات التشريعات الأقل صرامةً.

وتأتي أكبر مخاوف مراقبـي الملكية الفكرية في عالم التقانة من الصين. فهي بصفتها موقعةً على جميع المعاهدات السابقة، تنطبق عليها جميع المعايير التي تنطبق على البلدان الأخرى، بما فيها الولايات المتحدة. وفي اجتماع منتدى التعاون الاقتصادي في آسيا والباسيفيك (آبيك) عام 2011، أخبر الرئيس الصيني، هو جنتاو، مجموعةً من قادة الأعمال بشكلٍ غير رسمي أن الصين "ستطبق جميع قوانين الملكية الفكرية التي تطالب بها منظمة التجارة العالمية وفقاً للمعايير الغربية الحديثة". وقد حضرنا هذا الاجتماع، وعند مغادرتنا للغرفة بعد تعليقات الرئيس هو، عبّر فريق الأعمال الأمريكي بوضوح عن شكّه في ادعاءاته، وكان لديه سببٌ وجيهٌ لذلك، حيث تشير التقديرات إلى أن الشركات الأمريكية قد خسرت حوالى 3.5 مليارات دولار عام 2009 فقط بسبب قرصنة التسجيلات الموسيقية والبرمجيات في الصين. وأن 79 بالمئة من جميع البضائع المخالفة لحقوق النشر التي أوقفت في الولايات المتحدة كانت منتجةً في الصين. ومن الواضح أن المشكلة لا تعود إلى غياب القوانين فقط، بل إلى التقاعس عن تطبيقها. فالقانون الصيني يمنع رسمياً إنتاج البضائع المزيفة أو نسخ المواد ذات الملكية الفكرية بهدف الربح. أما عملياً، لا يشجّع المسؤولون الملاحقة القضائية لهذه الجرائم، ويُسمح للمخترقين بالحفاظ على أرباحهم. علاوةً على ذلك، تُفرض غراماتٌ متدنيةٌ جداً، وبطريقةٍ متذبذبةٍ جداً،

إلى حدٍّ يبطل أثرها في الردع عن مثل هذا السلوك. كما أن الفساد المحلي، وعلى مستوى الولاية، يشجّع المسؤولين على غض أبصارهم وتجاهل الاختراقات المتكررة.

وليست الصين بأي حالٍ من الأحوال الدولة الوحيدة غير الراغبة أو العاجزة عن تطبيق معايير الملكية الفكرية الدولية. فروسيا والهند وباكستان معروفةٌ جميعها بتطبيقها القاصر لهذه القوانين بالطريقة نفسها، وإذا كانت إسرائيل وكندا لا تعتبران بيئتين راعيتين لانتهاكات حقوق الملكية الفكرية، فإن أياً من هذين البلدين لم يطبق معايير منظمة حقوق الملكية الفكرية العالمية وقوانينها؛ مما جعلهما ملاذاً للقرصنة على الإنترنت. وحتى ضمن مجموعة الدول التي توفر حمايةً شديدة لحقوق الملكية الفكرية، تبرز عادةً اختلافاتٌ لا يستهان بها في التفسير يمكن استغلالها. ففكرة الاستخدام العادل (وفقاً لصياغة الولايات المتحدة) أو التعامل العادل (كما يسميه البريطانيون) الذي يسمح باستخدامٍ محدود للمواد ذات حقوق الملكية الفكرية من دون موافقة حامل هذه الحقوق، تطبقّ في الاتحاد الأوروبـي بتشددٍ أعلى بكثير مقارنةً بكلٍّ من الولايات المتحدة والمملكة المتحدة.

الدول الافتراضية

نسمع كثيراً أن العالم الافتراضي يجعل الحجم أقل أهمية. فالتقانة تمكّن جميع الأطراف، وتسمح للفاعلين الأصغر حجماً بترك آثار أكبر من حجومهم، وليس على هؤلاء الفاعلين أن يكونوا معروفين أو ممثلين رسميين، بل إننا نعتقد أنه قد يحدث في المستقبل أن تتواجد دولٌ افتراضية تهزّ المشهد الافتراضي للدول المادية. فثمة اليوم في العالم المئات من الحركات الانفصالية - العنيفة وغير العنيفة - الفاعلة، وليس من الوارد أن يتغير ذلك في المستقبل. ويدفع معظم هذه الحركات شعورٌ بالتمييز الإثني أو الديني، وسنناقش قريباً كيف سيتجسد التمييز الفيزيائي والاضطهاد ضد هذه المجموعات في العالم الشبكي؛ مغيراً شكله من دون أن يغير غايته. فليس غريباً في العالم المادي على مجموعاتٍ مضطهدة أن تتعرض لقوانين تمييزية، أو أن تقع ضحية الاعتقال التعسفي والإعدام من دون محاكمة، وأن تحرم من المحاكمات اللائقة، إضافة إلى جميع أشكال القيود على حرياتها المدنية والإنسانية. وستجد معظم هذه الوسائل طريقها إلى الشبكة بمعونةٍ كبيرة من التقانة التي تساعد الأنظمة على مراقبة الأقليات المتململة من شعوبها ومضايقتها واستهدافها.

قد تختار المجموعات التي لا تمتلك دولة رسمية، عندما تصبح محاصرةً في كلا العالمين المادي والافتراضي، أن تحاكي هذه الدولة على الشبكة. ففي حين لا يتمتع هذا التكوين بالشرعية والفائدة التي يتمتع بها تكوين الدولة الفعلي، فإن فرصة إقامة السيادة افتراضياً قد يثبت أنها - في أفضل الأحوال - خطوةٌ لا يستهان بها على طريق تحقيق تكوين دولةٍ رسمي أو - في أسوأ الأحوال - تصعيدٌ يعمّق الهوة بين الطرفين؛ وصولاً إلى صراعٍ أهليٍّ منفلت. فقد يبني أكراد إيران وتركيا وسوريا والعراق (وهي البلدان الأربعة التي يتركزون فيها) شبكة وب كردية كطريقةٍ لإحداث

شكلٍ من أشكال الاستقلال الافتراضي. وبما أن كردستان العراق يتمتع بالحكم الذاتي بمعنىً من المعاني، فقد تبدأ هذه المساعي هناك. وقد يؤسس الأكراد نطاق أسماء جذريًّا (مثل www أو .com) ينتهي بـ kurd ويرمز لكردستان، عبر تسجيل هذا النطاق وإقامة المخدمات في بلدٍ حيادي أو داعم لهم، ثم يتابعون البناء على هذا الأساس.

لن تقتصر الدولة الافتراضية على مجرد إشارةٍ واسم نطاق، فثمة مشاريع إضافية من شأنها أن تطور الحضور الكردي وتميزه على الشبكة. وإذا بذل ما يكفي من الجهود، يمكن لشبكة الوب الكردية أن تصبح نسخةً مستقرة من الإنترنت الخاصة بدولٍ أخرى، لكن باللغة الكردية بالطبع. وبناءً على ذلك، يستطيع المهندسون الأكراد أو المتعاطفون معهم بناء تطبيقات وقواعد بيانات وغيرها من المواقع الشبكية التي لا تدعم القضية الكردية وحسب، وإنما تسهلها بشكلٍ ميداني أيضاً. ويمكن للوسط الكردي الافتراضي أن ينظم الانتخابات، وينشئ الوزارات لتوصيل البضائع العامة الأساسية. بل ويمكنهم أيضاً استخدام عملة افتراضية فريدة. ويستطيع الوزير الافتراضي للمعلومات أن يدير تدفق البيانات من وإلى

الأكراد على الشبكة، بينما يركز وزير الداخلية على الحفاظ على أمن الدولة الافتراضية وحمايتها من الهجومات السايبرية، وقد ينخرط وزير الخارجية في علاقاتٍ دبلوماسية مع دولٍ أخرى حقيقية، فيما يروج وزير الاقتصاد والتجارة للتجارة الإلكترونية بين الأوساط الكردية والمصالح الاقتصادية الخارجية.

تماماً كما تتعرض المحاولات الانفصالية الساعية لتأسيس دولة مادية إلى ممانعة الدولة المضيفة عادةً، ستواجه مثل هذه المجموعات معارضةً مشابهة للمناورات التي تقوم بها على الشبكة. فإنتاج شيشان افتراضية قد يقوي التضامن الإثني والسياسي بين داعميها في منطقة القوقاز، لكنه سيؤدي بلا شك إلى تردي العلاقات مع الحكومة الروسية التي ترى في مثل هذه الخطوة انتهاكاً لسيادتها. وقد يستجيب الكرملين بدوره لهذا الاستفزاز الافتراضي بحملةٍ مادية، فيرسل دباباته وقواته لقمع الاضطرابات في الشيشان.

أما بالنسبة إلى الأكراد المنتشرين عبر دولٍ متعددة، فسيحدق بهم هذا الخطر على نحوٍ أكثر وضوحاً. حيث ستواجه الحملة الكردية لتأسيس دولةٍ افتراضية ممانعة منطقة كاملة - بعض دولها لا تعيش فيها جاليةٌ كردية - لكنها ستخشى أثرها على الاستقرار، ولن تُدّخر أية جهود لتدمير المؤسسات الافتراضية الكردية، عبر التدخل السايبري البدائي والتجسس؛ كالهجومات السايبرية وحملات التضليل والتسريب. ولا شك في أن الشعب على الأرض هو الذي سيتحمل عبء العقوبات. وستجد الحكومات خير عونٍ لها في مقادير البيانات الهائلة التي ينتجها هؤلاء المواطنون بالطبع؛ حيث سيسهل عليها إيجاد أولئك المتورطين في الدولة الافتراضية أو الداعمين لها. وقليلةٌ هي الحركات الانفصالية التي يتوفر لها المستوى اللازم من الموارد والدعم الدولي لمواجهة هذا الهجوم المعادي.

سيصبح إعلان دولة افتراضية جريمة خيانةٍ عظمى؛ ليس فقط في المناطق القاسية، وإنما في كل مكان. فهي طريقٌ أكثر خطورةً من أن تترك مفتوحةً،

ومفهوم المؤسسات الافتراضية وحده كفيلٌ بأن يبعث الحياة في المجموعات الانفصالية التي حاولت وفشلت في التوصل إلى نتائج ملموسة بالوسائل العنيفة، كما حدث مع انفصاليي الباسك في إسبانيا، والوطنيين الأبخاز في جورجيا أو جبهة التحرية الإسلامية لشعب المورو في الفلبين. وقد تكون محاولةٌ فاشلة أو غير مناسبة كفيلةً بتحطيم التجربة برمتها. فلو حشد الداعمون المترددون لحركة انفصالية في تكساس على سبيل المثال قواهم لإطلاق جمهورية تكساس الافتراضية على سبيل المثال، وقوبلوا بالسخرية، فسيشوه ذلك مفهومَ الدولة الافتراضية لبعض الوقت. ويبقى أن نرى مدى النجاح الذي ستحققه محاولات الدول الافتراضية هذه، (وما هو معيار النجاح في النهاية)، لكن مجرد وجود جدوى محتملة منها مؤشّر مهمّ على تحلل سلطة الدولة في العصر الرقمي.

الاستفزاز الرقمي والحرب السايبرية

لن تكتمل مناقشة مستقبل الدول في عصر الاتصالات من دون إلقاء نظرة على أسوأ ما ستقوم به ضد بعضها؛ أي الحروب السايبرية. لا تعتبر الحرب السايبرية مفهوماً جديداً، لكن معاملاتها ليست معروفة جيداً. ولا ينفك خبراء أمن الحاسب يتجادلون حول حجم الخطر المحدق، وماهيته، وحول تحديد ما يمكن اعتباره حرباً سايبرية بالفعل. أما نحن فنستخدم تعريف الحرب السايبرية الذي يقدمه رئيس وحدة مكافحة الإرهاب الأمريكية السابق، ريتشارد كلارك، الذي يصفها بأنها "مبادرة دولة قومية ما إلى اختراق حواسب دولة أخرى وشبكاتها بغرض إلحاق الضرر بها أو إثارة الاضطراب فيها".

إن الهجمات السايبرية (كالتجسس الرقمي، والتخريب، والتسلل، وغيرها من أشكال الأذى) كما بيّنّا سابقاً، صعبة الملاحقة، وتهدف إلى إلحاق ضرر جسيم عادة. وستلجأ المجموعات الإرهابية والدول على حدٍّ سواء إلى استغلال وسائل الحرب السايبرية[*]، وإن كانت الحكومات ستركز أكثر على جمع المعلومات وليس على التدمير الصريح. وستكون الحرب السايبرية بالنسبة للدول تحقيقاً لغايات استخباراتية، وإن كانت الطرائق المستخدمة شبيهة بتلك التي يطبقها الفاعلون المستقلون الذين يسعون إلى إثارة المتاعب. فسرقة الأسرار التجارية، والوصول إلى المعلومات السرية، والتسلل إلى أنظمة الحكومة، ونشر المعلومات المضللة، جميعها أنشطة تقليدية لوكالات الاستخبارات. وهي ستشكل الجزء الأعظم من الهجمات السايبرية بين الدول في المستقبل.

لكن الكثيرين يختلفون معنا جذرياً في هذه النقطة، فيتوقعون بدلاً من ذلك أن تسعى الدول إلى تدمير أعدائها بطرائق ثقيلة اليد، مثل قطع شبكات الطاقة عن بعد، أو تحطيم أسواق الأسهم. ففي شهر تشرين الأول من عام 2012 حذّر وزير الدفاع في الولايات المتحدة ليون بانيتا من أن "دولة معتدية... قد تستخدم هذه الأنواع من الأدوات السايبرية لتسيطر على المفاصل الحيوية. وقد تتمكن عندها من إخراج قطارات الركاب عن مساراتها أو حتى - وهذا أخطر - إخراج قطارات ركاب محملة بالمواد الكيميائية عن مساراتها. وربما تقوم بتلويث المياه في المدن

الكبرى، أو إغلاق شبكة الطاقة في أجزاء كبيرة من البلاد". لكننا نميل إلى وجهة النظر المتفائلة (على الأقل في ما يتعلق بالدول)، ونقول إن مثل هذه التصعيدات - وإن كانت ممكنة - غير واردة. ويكفي أن الحكومة التي تبدأ بمثل هذا التوجه ستتحول بنفسها إلى هدف، لتصبح عبرة يعتبر بها حتى أكثر النظم شذوذاً.

ومن العدل القول إننا نعيش منذ اليوم في عصر حرب سايبرية تقودها الدول، وإن كان معظمنا غير مدرك لذلك. فبينما أنتَ تقرأ هذه السطور، ربما تكون حكومة بلد أجنبـي تخترق قواعد بيانات حكومتك لتدمر مخدماتها، أو لتراقب محادثاتها. وقد تبدو المرحلة التي نحن فيها من الحرب السايبرية بالنسبة لمراقبين خارجيين مرحلة لطيفة، بل إن البعض قد يجادل بالفعل بالقول إنها ليست حرباً حقيقية على أية حال؛ وفقاً لإطار كلاوزفيتس الذي يعتبر الحرب "متابعةً للسياسة بطريقة أخرى". فقد يحاول المهندسون المدعومون من قبل الحكومة التسلل إلى نظم المعلومات الخاصة بشركات البلدان الأخرى ومؤسساتها وإغلاقها، لكن أحداً لن يتعرض للقتل أو الجرح. وقد رأينا قدراً بسيطاً من نُذُر هذه الحروب السايبرية في العالم المادي إلى درجة أن المدنيين يرون في الهجوم السايبري إزعاجاً أكثر منه تهديداً؛ مثل موجة من الزكام.

لكن، على أولئك الذين يقللون من شأن التهديد الذي تمثله الحرب السايبرية أن يتحملوا بأنفسهم عواقب هذا التهاون. فعلى الرغم من أن الهالة التي تحيط بالحرب السايبرية ليست مبررة دائماً، إلاّ أنّ المخاطر التي تفرضها حقيقة قائمة. والهجومات السايبرية تحدث بتكرار متزايد وبدقة تتعاظم بمرور كل عام. والتواصل المتزايد في حياتنا مع نظم المعلومات الرقمية يجعلنا أضعف مع كل نقرة جديدة. ومع دخول الكثير من البلدان الجديدة إلى الإنترنت في المستقبل القريب ستكبر نقاط الضعف هذه وتصبح أكثر تعقيداً.

قد يكون الهجوم السايبري هو السلاح المثالي للدولة. فهو قوي، ويمكن تخصيصه، ولا يفضح هوية مرتكبه. فالاختراق، ونشر الديدان الحاسوبية، وأحصنة طروادة، وغيرها من وسائل التجسس الافتراضي، تقدم للدولة مدىً أوسع وتغطية أكبر مما يمكنها تحقيقه عبر الأسلحة التقليدية والعمليات الاستخباراتية. وآثار الجريمة هنا تتلاشى بسرعة؛ مما يؤمن لمرتكبيها تمويهاً فعالاً، ويحد من قدرة الضحايا على الاستجابة. وحتى إذا أمكن تتبع الهجوم والوصول إلى منطقة أو مدينة معينة، فإن تحديد الأطراف المسؤولة عنه يكاد يكون مستحيلاً. فكيف لبلد أن يحدد الاستجابة المناسبة إذا كان عاجزاً عن إثبات التهمة. ووفقاً لكريغ مندي، مسؤول الأبحاث والاستراتيجيات الرئيس في مايكروسوفت، والمفكر القيادي لأمن الإنترنت، فإن العجز عن تحديد الفاعل - وهو من المواضيع المألوفة لدينا - يجعل هذه الحرب تدار في الظلام. لأنه "من الصعوبة بمكان معرفة من أطلق النار عليك". ويسمي مندي وسائل التجسس السايبري "أسلحة التعطيل الشامل"، ويقول: "سيكون انتشارها أسرع بكثير، مما يجعل هذا النوع من الصراع أكثر خفاءً مقارنة بما يعتبر حرباً تقليدية".

ستتخذ الدول إجراءات ضد بعضها على الشبكة كانت ستعتبر استفزازات صارخة

خارجها، مما سيسمح بإدارة النـزاعات حتى نهايتها في الميدان الافتراضي، بينما يبقى كل شيء آخر هادئاً. وسيجعل إغفال الهوية شبه المحكم الهجومات السايبرية خياراً مفضلاً لدى البلدان التي لا تريد أن تبدو مفرطة في العنف، وترغب مع ذلك بالنيل من عدوها. وإلى أن تتحسن قدرات الخبراء التقنيين في تحديد مصادر الهجومات السايبرية، ويصبح القانون قادراً على محاسبة المذنبين، ربما سينغمس عدد أكبر من الدول في هذه النشاطات التي نشهدها اليوم. وستبدأ كتل كاملة من الدول التي تحصل اليوم على الاتصالات والقدرات التقنية في أمريكا اللاتينية وآسيا والشرق الأوسط بهجوماتها الخاصة قريباً؛ وإن كان ذلك من باب الاختبار فقط. وحتى إن تلك الدول التي تحتاج إلى القدرات التقنية (كالمهندسين والمخترقين المحليين)، ستجد طرقاً للحصول على الأدوات التي تحتاج إليها.

لكي نوضح كيف تبدو الحرب السايبرية الشاملة، سنأخذ بعض الأمثلة الحديثة. وربما كان أشهرها دودة ستوكسنيت التي تم اكتشافها عام 2010، والتي اعتبرت أكثر البرمجيات الخبيثة التي يُكشَف عنها تطوراً على الإطلاق؛ إلى أن اكتشف فيروس عرف باسم فليم عام 2012 ليستأثر باللقب. وقد اكتُشف أن دودة ستوكسنيت، المصممة لمهاجمة نوع معين من نظم التحكم الصناعي العاملة على نظام التشغيل ويندوز، قد تسللت إلى نظم المراقبة في منشأة ناتانـز للإخصاب النووي بإيران، وتسبّبت بتسارع أجهزة الطرد فجأة، وتباطُئها حتى تصل إلى مرحلة التدمير الذاتي على التوازي مع تعطيل أنظمة الإنذار. وبما أن النظم الإيرانية ليست متصلة بالإنترنت، فلا بد أن الدودة قد تم تحميلها مباشرة، فربما أدخلها موظف من دون قصد بواسطة قرص تخزين ومضي. ثم تمّ بعد ذلك سد الثغرات في نظم ويندوز، لكن بعد أن ألحقت الضرر بالمشاريع النووية الإيرانية، كما اعترف الرئيس الإيراني محمد أحمدي نجاد.

لم تكن الجهود المبذولة لتحديد معدّي الدودة حاسمة، ولو أنّ الاعتقاد الأكثر شيوعاً هو أنها نتيجة تجارب مدعومة من قبل دولة ما؛ نظراً إلى مستوى تعقيدها والهدف الذي صممت من أجله. ومن بين ما دفع نحو هذا الاعتقاد ما لاحظه المحللون الأمنيون الذين شرّحوا الدودة (والذين تمكنوا من إجراء تجاربهم بفضل خروج ستوكسنيت "إلى البرية"، أي خارج وحدة ناتانـز) ضمن الشيفرة المصدرية من إشارات إلى تواريخ وقصص من الكتاب المقدس ذات رمزية كبيرة بالنسبة للإسرائيليين. (لكن آخرين رأوا أن هذه المؤشرات كانت مباشرة إلى حد يجعلها حججاً مزيفة). وتشير الموارد المستخدمة أيضاً إلى إنتاج حكومي، حيث يعتقد الخبراء أن الدودة قد كتبت من قبل ما لا يقل عن ثلاثين شخصاً على مدى شهور عدة. وهي تستخدم عدداً غير مسبوق من ثغرات "اليوم صفر"، وهي هجومات حاسوبية خبيثة تستغل نقاط ضعف (ثغرات حاسوبية) في البرامج الحاسوبية لم تكن معروفة لمصممي البرامج (كما في حالة نظام التشغيل ويندوز) قبل يوم الهجوم؛ مما لا يترك لهم أي وقت للتحضر له. ويعتبر اكتشاف ثغرة "اليوم صفر" واحدة حدثاً نادراً، ويمكن بيع المعلومات المسروقة مقابل مئات الآلاف من الدولارات في السوق السوداء، لذا دهش المحللون الأمنيون من نسخة مبكرة من

ستوكسنيت كانت تستغل خمساً من هذه الثغرات.

وبالطبع، كشف النقاب في حزيران من عام 2012 عن أن حكومتين وليست حكومة واحدة كانتا تقفان خلف دودة ستوكسنيت. وقد أكد مسؤولون في إدارة أوباما لمراسل نيويورك تايمز ديفيد إي.سنجر، من دون أن تتم تسميتهم، أن دودة ستوكسنيت كانت مشروعاً مشتركاً أمريكياً إسرائيلياً مصمماً لشل برنامج الأسلحة النووية الإيراني المشتبه به وتعطيله*. وكانت المبادرة التي أخذت الضوء الأخضر الأولي في عهد الرئيس جورج دبليو بوش تحت الاسم المرمز "الألعاب الأولمبية"، قد انتقلت إلى الإدارة التالية ليقوم الرئيس أوباما بتسريعها؛ حيث سمح شخصياً بمتابعة تطوير هذا السلاح السايبري. وبعد بناء هذه الدودة الخبيثة واختبارها على مستنسخات قيد التشغيل لمحطة ناتانـز تم بناؤها في الولايات المتحدة، وبعد أن ثبت أنها قادرة بالفعل على التسبب بانهيار أجهزة الطرد، وافقت حكومة الولايات المتحدة على نشر الدودة. ولم يكن لأهمية هذه الخطوة أثر كبير على المسؤولين الأمريكيين. فكما قال ميشيل في.هايدن، المدير السابق للسي.آي.أيه، لسنجر فإن "الهجومات السايبرية السابقة كانت تنحصر بالحواسب. وهذا هو الهجوم الأول على هذا المستوى الذي يتم فيه استخدام هجوم سايبري للتسبب بتدمير مادي فعلي. ثمة من تجاوز نقطة العودة!".

وعندما تم اكتشاف فيروس فليم بعد مرور عامين، أشارت التقارير الأولية الصادرة عن محللين أمنيين إلى عدم صلته بستوكسنيت، فقد كان أكبر بكثير، ويستخدم لغة برمجة مختلفة، ويعمل على نحو مختلف. حيث كان يركز على جمع المعلومات سراً بدلاً من استهداف أجهزة الطرد. وكان الفيروس أكثر قدماً أيضاً، فقد اكتشف أحد المحللين أن فليم كان موجوداً منذ أربع سنوات ماضية على الأقل عندما تم اكتشافه، أي إن تاريخه يسبق تاريخ ستوكسنيت. وأفاد سنجر أن المسؤولين الأمريكيين أنكروا أن فليم جزء من مشروع الألعاب الأولمبية. إلاّ أنه لم يمض سوى شهر واحد على الإفشاء عن هذه الأسلحة السايبرية علناً حتى توصل خبراء الأمن في مختبر كاسبرسكي - وهو شركة أمن حواسب روسية ضخمة تتمتع بمصداقية دولية - إلى أن الفريقين اللذين قاما بتطوير ستوكسنيت وفليم قد تعاونا بالفعل في مرحلة مبكرة. وقد حددوا وحدة برمجية معينة تعرف باسم المورد 207 كانت موجودة في دودة ستوكسنيت وتحتوي على شيفرات برمجية من الواضح أنها مشتركة مع فليم. "يبدو وكأن منصة فليم كانت بمثابة نقطة الانطلاق للمضي في مشروع ستوكسنيت"، كما يوضح أحد كبار الباحثين في مركز كاسبرسكي. "وقد تمت متابعة العمليات بمسارات مختلفة؛ ربما لأن شيفرة ستوكسنيت البرمجية قد بلغت حداً كافياً من النضوج يسمح بنشرها "في البرية". ونحن اليوم على يقين تام بأن مجموعتي ستوكسنيت وفليم قد عملتا معاً".

مع أن ستوكسنيت وفليم وغيرهما من الأسلحة السايبرية المرتبطة بالولايات المتحدة وإسرائيل تعتبر الأمثلة الأكثر تطوراً للهجومات السايبرية التي ترعاها الدولة، فإن طرائق أخرى للحرب السايبرية قد تم استخدامها مسبقاً من قبل الحكومات حول العالم. وليس من الضروري أن تنحصر هذه الهجومات بمسائل

جيوسياسية ذات عواقب كبرى، فقد يتم اللجوء إليها لإزعاج دولة ند مكروهة بمستوى المهارة نفسه. فبعد الخلاف الدبلوماسي حول قرار حكومة أستونيا عام 2009 بإزالة النصب التذكاري الروسي للحرب العالمية الثانية من عاصمتها تالين، تعرضت مجموعة من مواقع الوب الأستونية الكبرى، بما فيها البنوك والصحف والمؤسسات الحكومية، إلى هجوم حجب خدمة موزع مباغت. وأستونيا كثيراً ما تسمى البلد الأكثر اتصالاً على وجه الأرض؛ لأن كل وظيفة من الوظائف اليومية فيها تقريباً (وجميع مواطنيها تقريباً) تستخدم خدمات شبكية، بما فيها الحكومة الإلكترونية، والتصويت الإلكتروني، والصيرفة الإلكترونية، والمواقف التي تسمح للسائقين بدفع رسوم المواقف عبر الأجهزة النقالة. إلا أن البلد الذي منح العالم خدمة سكايب وجد نفسه فجأة مشلولاً نتيجة محاولات مجموعة من المخترقين. وعادت هذه النظم إلى العمل على الشبكة، لكن الأستونيين شكوا مباشرة بجيرانهم الروس. واتهم وزير الخارجية الأستوني الكرملين مباشرة، لكنْ لم يكن من الممكن إثبات هذه التهم. وقد عجز خبراء المفوضية الأوروبية والناتو عن إيجاد دليل على تورط الحكومة الروسية رسمياً (أما الروس من جهتهم فقد أنكروا هذه التهم).

تحدى لاري كونستانتين، البروفيسور في جامعة ماديرا في البرتغال، تحليلات سنجر في مقابلة له في الرابع من أيلول عام 2012 أجريت بطريقة بودكاست مع ستيفين شيري، أحد كبار المحللين الزملاء في مجلة سبيكتروم الصادرة عن معهد آي.إي.إي؛ معهد المهندسين الإلكترونيين والكهربائيين، قائلاً إنه من المستحيل تقنياً أن ينتشر ستوكسنيت بالطريقة التي شرحها سنجر (أي إن ستوكسنيت لا يستطيع الانتشار سوى في شبكة محلية وليس عبر الإنترنت). ونحن نرى أن حجة كونستانتين تملك من المصداقية ما يكفي لمناقشتها على الأقل.

ويبرز هنا سؤالان (فما الذي يعتبر إعلان حرب سايبرية؟ وهل يعتبر قيام الكرملين ليس بأمر المخترقين، وإنما بمباركة أعمالهم فقط حرباً سايبرية؟) لكنّ هذين السؤالين يبقيان من دون إجابة. فمع العجز عن تحديد الفاعل، يبقى ضحايا الهجمات السايبرية بلا حيلة، وقد يبقى المهاجمون في مأمن من الملاحقة حتى مع ارتفاع مقدار الشك فيهم (فبعد عام على الهجومات على أستونيا، تم تعطيل مواقع وب تابعة للحكومة والجيش الجورجيين عبر هجومات حجب خدمة موزعة، حين كانت البلاد على خلاف مع - ربما حزرت بنفسك - روسيا. وفي العام التالي، استهدف المخترقون الروس مزودات الإنترنت في قرغيزستان، فأغلقوا 80 بالمئة من عرض الحزمة المتوفر في البلاد لمدة أيام. ويعتقد البعض أن الهجومات كانت تهدف إلى لجم الحزب المعارض هناك، والذي كان يتمتع بحضور كبير نسبياً على الإنترنت. في حين يزعم آخرون أن الدافع وراء الهجوم كان صفقة استثمار فاشلة حاولت روسيا عبرها دفع قرغيزستان إلى إغلاق القاعدة الأمريكية التي تستضيفها).

من دون أن ننسى الهجومات السايبرية الصينية على غوغل وعلى الشركات الأمريكية على مدى السنوات القليلة المنصرمة. فالتجسس التجاري الرقمي فئة غنية من فئات الحروب السايبرية، ويعتبر ظاهرة جديدة نسبياً. لكن، سيكون له في

المستقبل أثر كبير على العلاقات بين الدول، وعلى العلاقات بين الاقتصادات الوطنية. ويحدث كثيراً أن تجد غوغل أنظمتها عرضة لهجمات رقمية غير معروفة، وهو ما يدفعها إلى بناء شبكة تتمتع بأكبر حصانة ممكنة مع ما أمكن من وسائل الحماية لمستخدمي غوغل. وفي نهاية عام 2009، اكتشفت غوغل تدفقاً غير اعتيادي على شبكتها فبدأت بمراقبة هذا النشاط (كما يحدث في كثير من الهجومات السايبرية، كان الأنجع بالنسبة لخبرائنا في الأمن السايبري أن يتركوا القنوات المخترقة مفتوحةً مؤقتاً حيث تتسنى مراقبتها، بدلاً من إغلاقها مباشرة). وما تم اكتشافه كان هجوماً صناعياً متطوراً إلى حد كبير على الملكية الفكرية لغوغل قادماً من الصين.

وخلال التحريات التي قامت بها غوغل، تم جمع ما يكفي من الأدلة التي تثبت أن الحكومة الصينية - أو عملاءها - كانت تقف وراء الهجوم. وبعيداً عن الأدلة التقانية، كانت الهجومات تشتمل في جزء منها على محاولات للوصول إلى حسابات البريد الإلكتروني جي.ميل الخاصة بناشطين صينيين في حقوق الإنسان ومراقبتها، إضافة إلى حسابات مدافعين عن حقوق الإنسان في الصين مقيمين في الولايات المتحدة وأوروبا (كانت معظم هذه الهجومات قد باءت بالفشل). وفي النهاية، كان هذا الهجوم (الذي لم يستهدف غوغل فقط، وإنما العشرات من الشركات الأخرى المدرجة علناً) أحد العوامل التي دفعت غوغل إلى اتخاذ قرار بتغيير موقعها التجاري في الصين؛ الأمر الذي نتج عنه إغلاق أعمال غوغل الصيني، ونهاية الرقابة الذاتية لمحتوى الإنترنت الصيني، وتحويل جميع عمليات البحث الداخلة إلى غوغل في هونغ كونغ.

قليلة هي اليوم الدول القادرة على شن هجومات سايبرية واسعة النطاق (حيث يقف غياب الشبكات السريعة والمواهب التقنية عائقاً أمام غيرها)، لكن عشرات الدول الأخرى ستبدي المزيد من المشاركة في المستقبل، سواء أفعلت ذلك هجومياً أم دفاعياً. ويعتقد كثيرون أن سباق التسلح الجديد قد بدأ بالفعل، حيث تخصص الولايات المتحدة والصين وإسرائيل وإيران وغيرها استثمارات كبيرة لجمع القدرات التقانية والمحافظة على موقعها التنافسي في هذا المجال. ففي عام 2009، في الوقت نفسه الذي أعطى فيه البنتاغون الأمر بتأسيس الآمرية السايبرية الأمريكية (يو.إس سايبر كوم) تقريباً، أعلن روبرت غيتس، وزير الدفاع آنذاك، أنّ الفضاء السايبري هو "النطاق الخامس" للعمليات العسكرية؛ إلى جانب البر والبحر والجو والفضاء. وربما يقوم الجيش في المستقبل بابتكار مكافئ سايبري لقوة ديلتا العسكرية، أو قد نشهد تأسيس قسم الحرب السايبرية مع حقيبة وزارية جديدة. وإذا كنت تجد هذا مبالغاً فيه، فتذكر أن إنشاء قسم الأمن الوطني جاء رداً على أحداث الحادي عشر من أيلول؛ فكل ما يتطلبه الأمر حدث قومي جلل يحفز مبادرة كبيرة من قبل الحكومة مع تخصيص الموارد اللازمة لها. وتذكر أن تجربة المملكة المتحدة مع الإرهاب الإيرلندي هي التي أدت إلى وضع كاميرات التلفزة مغلقة الدارة (سي.سي.تي.في) في كل ركن في لندن، في حركة لاقت ترحيباً لدى شرائح عريضة من الشعب لديها بالطبع مخاوف من التسجيل المصور لجميع تحركاتها في

الشوارع وتخزينها، لكن لحظات الطوارئ الوطنية تفرض دوماً أن يسود الصقور على الحمائم. فالإجراءات الأمنية لما بعد الأزمة باهظة التكاليف؛ حيث يتوجب على الدولة أن تتصرف بسرعة، وأن تقطع شوطاً إضافياً لتهدئة مخاوف شعبها. ويقدر بعض خبراء الأمن السايبري تكاليف "المجمع الصناعي - السايبري" الجديد بما بين 80 إلى 150 مليار دولار سنوياً.

تمتلك البلدان ذات القطاعات الهندسية القوية مثل الولايات المتحدة ما يكفي من رأس المال البشري لبناء أسلحتها الافتراضية "من-زلياً". لكن، ماذا عن الدول التي لا تمتلك شعوبها القدرات التقنية المتطورة؟ لقد سبق أن مررنا بتجارة المعادن مقابل التقانة التي تلجأ إليها الحكومات الساعية لبناء دول رقابية، ومن المنطقي أن تلاقي هذه المقايضة النجاح نفسه عندما يتحول اهتمام هذه الدول إلى أعدائها الخارجيين. فستجد دولٌ في أفريقيا وأمريكا اللاتينية وآسيا الوسطى دولاً مزودة يمكن لاستثماراتها التقانية أن ترفع مستوى البنية التحتية التي تحتاج إلى الأولى. وستكون الصين والولايات المتحدة الأمريكية أكبر مزودَين، لكنهما لن تكونا الوحيدتين بأي حال من الأحوال؛ حيث ستتنافس الوكالات الحكومية والشركات الخاصة من جميع أنحاء العالم على عرض المنتجات والخدمات على البلدان الراغبة بحيازتها. وستتم معظم هذه الصفقات من دون معرفة شعوب أي من هذه البلدان؛ مما سيقود إلى طرح بعض الأسئلة غير المريحة إذا كشف النقاب عن الشراكة القائمة. ففي مداهمة لبناء أمن الدولة المصري بعد الثورة التي قامت في البلاد عام 2011 تم الكشف عن عقود فضائحية مع أسواق خاصة، كان من بينها عقد مع شركة بريطانية مغفلة الهوية كانت تبيع برمجيات تجسس شبكية لنظام مبارك.

سيكون اختيار البلد المصدر قراراً هاماً بالنسبة للبلدان التي تتطلع إلى تطوير قدراتها في الحرب السايبرية؛ فهو بمثابة الموافقة على الوقوع في "دائرة النفوذ الافتراضي" لهذا البلد. وستضغط الدول المزوِّدة بقوة لتضمن موطئ قدم لها في الدول الناشئة؛ لأن هذه الاستثمارات تشتري النفوذ. وقد حققت الصين نجاحاً لافتاً في توسيع تواجدها في أفريقيا، حيث تقايض المساعدة التقنية ومشاريع البنى التحتية الكبرى بالموارد وأسواق المستهلكين؛ في ما يعود في جزء لا يستهان به إلى سياسة عدم التدخل الصينية وعروضها المنافسة. فإلى أي بلد يرجح أن تلجأ البلدان التي تتطلع إلى تطوير قدراتها عندما تقرر الشروع ببناء ترسانتها السايبرية؟

إننا نشاهد بالفعل مؤشرات على استثمارات مشابهة تجري تحت مظلة مشاريع التنمية العلمية والتقانية. فتان-زانيا - الدولة الاشتراكية السابقة - إحدى الدول الكبرى التي تتلقى المساعدة الخارجية المباشرة من الصين. ففي عام 2007، عُهد إلى شركة الاتصالات الصينية بمد حوالى 10,000 كم من كابلات الألياف الضوئية. وبعد ذلك بعدة سنوات، أعلنت شركة مناجم صينية تدعى سيشوان هونغدا أنها أبرمت صفقة بقيمة 3 مليارات دولار مع تان-زانيا لاستخراج الفحم والحديد الخام من جنوب البلاد. وبعد ذلك بوقت قصير، أعلنت الحكومة التان-زانية أنها أبرمت اتفاقية إقراض مع الصين لبناء خط أنابيب غاز طبيعي بكلفة مليار دولار. وفي طول

القارة وعرضها، نجد علاقات تكافلية مشابهة بين الحكومات الأفريقية والشركات الصينية الكبرى التي تعود ملكية معظمها إلى الدولة (تمثل الشركات المملوكة للدولة 80 بالمئة من قيمة سوق الأسهم في الصين). فمن قرض بقيمة 150 مليون دولار لمشروع الحكومة الإلكترونية في غانا ستنفذه شركة هواوي الصينية، إلى مشفى بحثي في كينيا، و"المدينة التقانية الأفريقية" في الخرطوم؛ كلها مشاريع تلت منتدى التعاون الصيني الأفريقي (فوكاك)، وهو هيئة تم تأسيسها عام 2000 لتسهيل الشراكات الأفريقية الصينية.

ستسعى الدول الكبرى المزودة في المستقبل إلى بناء فضاءات نفوذها الافتراضي بناءً على بروتوكولات ومنتجات محددة؛ حيث تشكل تقاناتها العمود الفقري لمجتمع معين، وتصبح الدول الخاضعة لها معتمدة على بنى تحتية هامة تكون القوى العظمى هي الوحيدة التي تبنيها وتخدمها وتسيطر عليها. فاليوم، ثمة أربع شركات رئيسة مصنّعة لتجهيزات الاتصالات؛ وهي إيريكسون السويدية وهواوي الصينية وألكاتيل لوسنت الفرنسية وسيسكو الأمريكية. ولا شك في أن الصين ستستفيد من استخدام أجزاء كبيرة من العالم للتجهيزات والبرمجيات التي تقدمها لأن الحكومة الصينية تتمتع بنفوذ كبير على ما تقوم به شركاتها. فعندما تكسب هواوي حصة في السوق، ينمو نفوذ الصين وانتشارها أيضاً. أما إيريكسون وسيسكو فهما أقل خضوعاً لحكومتيهما. لكن، لا بد من أن يحلّ الوقت الذي تتوافق أو تتعارض فيه مصالح هواوي التجارية والوطنية مع الصين؛ ربما بسبب إساءة استخدام منتجاتها من قبل دولة مستبدة، وستقوم عندها بتنسيق جهودها مع حكوماتها على المستويين الدبلوماسي والتقني.

ستكون دوائر النفوذ الافتراضي هذه ذات طبيعة تقنية وسياسية في آن معاً. وإذا كانت هذه العلاقات عالية المستوى فقد لا تؤثر على الحياة اليومية للمواطنين عملياً، فما إن يطرأ شيء جدي (مثل تمرد يتم تنظيمه عبر الهواتف النقالة)، حتى يصبح هناك دور هام للتقانة التي تستخدمها البلاد ولدائرة النفوذ التي تقع فيها. فشركات التقانة تصدر قيمها إلى جانب منتجاتها، لذا إن لهويّة من يؤسس البنية التحتية للاتصالات أهمية بالغة. وثمة مواقف مختلفة إزاء النظم المفتوحة والمغلقة، ونقاشات حول دور الحكومة، ومعايير مختلفة للمحاسبة. فإذا قامت دولة خاضعة لنفوذ الصين على سبيل المثال بشراء التقانة لملاحقة المجموعات الأقلية الداخلية، فستكون قدرة الولايات المتحدة على التصرف محدودة جداً، وسيكون الحل القانوني بلا جدوى. إنها معركة تجارية ذات آثار أمنية عميقة.

حرب الشيفرة الجديدة

إن النتيجة المنطقية لدخول العديد من الدول الجديدة إلى الشبكة، وبنائها قدرات الهجوم السايبري أو شرائها لها، وعملها في دوائر متنافسة من النفوذ الشبكي، نشوبُ حرب سايبرية متدنية المستوى تكون مستمرة ولا تنتهي. فالدول الكبرى ستهاجم الدول الكبرى الأخرى؛ مباشرة أو عبر وكلاء، بينما ستستغل الدول النامية قدراتها الجديدة لتعالج مظالم قديمة لها. وستسعى الدول الصغرى إلى

تحقيق نفوذ أكبر من حجمها وهي مطمئنة إلى أنها لن تخضع للمحاسبة نظراً لطبيعة هذه الهجومات غير القابلة للتعقب. وبما أن معظم الهجومات ستكون عبارة عن تمارين جمع معلومات بطيئة الحركة وصامتة، فإنها لن تثير نقمة عنيفة؛ أي إن التوترات ستسخن على نار هادئة على مدى السنوات القادمة. وستقوم القوى العظمى ببناء جيوش افتراضية ضمن دوائر نفوذها؛ مضيفة طبقة وكلاء هامة تعزلها. وستكون قادرة عبر تعاونها على إنتاج الديدان والفيروسات، وعلى تنفيذ ضربات متطورة، إضافة إلى أشكال أخرى من التجسس الشبكي لتحقيق مكاسب تجارية وسياسية.

هذا ما يعتبره البعض حرب الشيفرة القادمة التي ستتورط فيها القوى الكبرى في حرب ضروس على أحد أبعادها، بينما يستمر التقدم الاقتصادي والسياسي في بعد آخر من دون أن يتأثرا. لكن هذا الصراع لن يكون كالحرب الباردة في العالم الحقيقي؛ أي لن يكون صراعاً بين طرفين بشكل أساسي، بل سيتحول إلى معركة متعددة الأقطاب مع مشاركة دول قوية تتمتع بالمعارف التقنية مثل إيران وإسرائيل وروسيا. وستبرز التصدعات الإيديولوجية واضحة على أساس حرية التعبير والبيانات المفتوحة والتحرر. وكما سبق وقلنا، إن قدراً قليلاً من هذا التصعيد سيجد طريقه إلى العالم المادي؛ لأن أياً من اللاعبين لن يرغب في تعريض علاقاته النامية للخطر.

ستنتقل بعض خصائص الحرب الباردة الكلاسيكية إلى حرب الشيفرة، وخصوصاً ما يتعلق بالتجسس، لأن الحكومات سترى في قدراتها الجديدة على خوض الحرب السايبرية امتدادات لوكالات استخباراتها قبل كل شيء. وبدلاً من حيل الخلد المتخفي والرسالة المسقطة وغيرها، ستُستخدم الديدان وبرمجيات رصد لوحة المفاتيح، والتتبع على أساس الموقع الجغرافي، وغيرها من أدوات التجسس الرقمي. وقد يؤدي استخراج المعلومات من الأقراص الصلبة بدلاً من استخراجها من البشر إلى تخفيض المخاطر التي تحيق بالأصول التقليدية وبالمتعاملين بها. لكنها ستفرض أيضاً تحديات جديدة؛ حيث ستبقى المعلومات المضللة مشكلة قائمة، وستكون الحواسب شديدة التطور أقل تساهلاً في إفشاء الأسرار مقارنة بالبشر.

وستنتعش صفة أخرى من صفات الحرب الباردة، وهي الحرب بالوكالة، في سياق تعقيدات العصر الرقمي الجديد هذه، وقد تتجسد في تحالفات تقدمية بين الدول لمواجهة عناصر خطيرة غير حكومية؛ مع توفر الغطاء السياسي نتيجة عدم إمكانية تحديد الفاعل. فيمكن للولايات المتحدة على سبيل المثال، أن تمول أو تدرب حكومات أمريكا اللاتينية، حيث تشن هذه الأخيرة هجوماتها الإلكترونية على شبكات تجار المخدرات. من جهة أخرى، قد تؤدي الحرب عبر وكيل رقمي إلى المزيد من أخطاء التوجه والاتهامات الباطلة، مع استغلال البلدان عدم إمكانية تحديد الفاعل لتحقيق مكاسب اقتصادية وسياسية.

وكما هو الأمر في الحرب الباردة، ستكون مشاركة المدنيين ومعرفتهم بما يجري والأضرار المباشرة الواقعة عليهم محدودةً، مما سيؤثر سلباً على تقدير الحكومات للمخاطر الناجمة عن مثل هذه النشاطات. فالدول الطموحة التي لا

تتمتع بالقدر الكافي من الخبرة في الأسلحة السايبرية قد تبالغ في مضيها وتولّد - من غير عمد - صراعاً يلحق الضرر بشعوبها بالفعل. وقد تظهر في النهاية مبادئ حتمية التدمير المتبادل بين الدول؛ مما يدفع هذه الديناميات إلى الاستقرار، لكن تعدد الأقطاب في المشهد ينذر ببقاء قدر ما من عدم الاستقرار في النظام.

والأهم من ذلك أنه سيكون هناك مجال كبير للخطأ في حرب الشيفرة الجديدة. فإساءة الفهم، وإساءة اختيار الطريق، وغيرها من الأخطار التي ميزت حقبة الحرب الباردة، ستظهر مجدداً وبقوة مع مضي المشاركين في عملية تعلم استخدام الأدوات الجديدة القوية التي أصبحت في متناولهم. فإذا أخذنا بعين الاعتبار الطبقة الإضافية من الإبهام التي تقدمها الهجمات السايبرية، فقد تكون النهاية أسوأ بعد من نهاية الحرب الباردة التي يمكن فيها تتبع آثار الصواريخ المنفجرة. وستُرتَكب الأخطاء من قبل الحكومات حين تحدّد أهدافها وطريقة استهدافها، ومن قبل الضحايا الذين سيثأرون من الطرف الخطأ نتيجة شعورهم بالذعر أو الغضب، ومن قبل المهندسين الذين سيبنون برامج الحاسب المعقدة الكبيرة هذه. فمع أسلحة بمثل هذا التعقيد التقني، من الممكن أن يقوم فرد سيّئ النية بتنصيب باب خلفي خاص به في البرنامج (وهي طريقة للولوج تتجاوز الآليات الأمنية، ويمكن استخدامها عن بعد) يبقى غير ملحوظ إلى أن يقرر استخدامه، أو ربما يقوم مستخدم من دون أن يعلم بمشاركة فيروس قوي البنية بطريقة لم يخطط لها مصنعو الفيروس؛ ليقوم الفيروس بتدمير سوق الأسهم في بلده بدلاً من مجرد تسريب معلومات حولها، أو قد يُكتشف برنامج خطير يحمل العديد من الرايات المزيفة (وهي النسخة الرقمية من الطعم) في شيفرته البرمجية، ليقرر البلد المستهدَف هذه المرة أن يتصرف إزاء المصدر الظاهري.

لقد سبق لنا أن رأينا أمثلة على كيفية اتخاذ الدولة للمسار الخاطئ نتيجة مشكلة تحديد الفاعل في الهجومات السايبرية. ففي عام 2009، أدت ثلاث موجات من هجومات حجب الخدمة الموزعة إلى شل مواقع وب حكومية كبرى في كل من الولايات المتحدة وكوريا الجنوبية. وعندما راجع الخبراء الهجوم السايبري وجدوا محتويات باللغة الكورية، إضافة إلى مؤشرات أخرى تشير بوضوح إلى أن شبكة الحواسب المهاجمة - أو الشبكة الروبوتية - قد انطلقت من كوريا الشمالية. وسارع المسؤولون في سيؤول إلى الإشارة بأصابعهم إلى بيونغ يانغ مباشرة. وقامت وسائل الإعلام الأمريكية بنقل القصة، وطالب مشرّع جمهوري بارز الرئيس أوباما بإجراء استعراض للقوة انتقاماً من كوريا الشمالية. إلا أن أحداً في الواقع لم يستطع أن يحدّد مصدر الهجومات بشكل قاطع، وبعد عام على ذلك، خلص المحللون إلى أنه ما من دليل على تورط كوريا الشمالية أو أية دولة أخرى. وكان محلل في فيتنام قد قال قبل ذلك إن الهجومات قد انطلقت من المملكة المتحدة، بينما أصر الكوريون الجنوبيون على أن وزارة الاتصالات الكورية الشمالية تقف خلفها. بل إن البعض ذهب إلى أن كل ما في الأمر مجرد خدعة حاكتها حكومة كوريا الجنوبية أو ناشطون، بهدف تحريض الولايات المتحدة على النظام في كوريا الشمالية.

لقد أجمعت معظم الروايات على أن هذه الهجمات كانت غير فعالة وغير متطورة (حيث لم تضِع أية بيانات، كما أن طريقة حجب الخدمة تعتبر سكيناً مثلمة)، وهو ما يفسر جزئياً سبب عدم حدوث تصعيد كبير. لكن، ماذا سيحدث عندما تمتلك بلدان جديدة القدرة على بناء ديدان ستوكسنيت، بل وأسلحة أكثر تطوراً بعد؟ وما هو الحد الذي يصبح عنده الهجوم السايبري إعلان حرب؟ وكيف يمكن لبلد ما أن يثأر إذا كان المهاجم قادراً في معظم الحالات على التخفي؟ سيكون على صانعي السياسات حول العالم الإجابة عن هذه الأسئلة في وقت أقرب مما يظنون. وثمة بعض الحلول لهذه التحديات، لكن معظم الخيارات - كإبرام اتفاقية دورية تتحكم بالهجمات السايبرية - ستتطلب استثمارات سخية، إضافة إلى الحوار الصريح حول ما يمكننا التحكم به وما لا يمكننا التحكم به.

غالباً، لن يكون تسلسل الأحداث الذي سيقود إلى هذه النقاشات مرتبطاً بحرب سايبرية بين الدول. بل من المرجح أن يكون الدافع هو التجسس التجاري المدعوم من قبل الدولة. حيث يمكن للدول احتواء سيل من الهجمات على شبكاتها الحكومية الخاصة، أما إذا استهدفت الشركات فستكون الهجومات أكثر علنية، وقد تؤثر على عدد أكبر من الناس إذا اشتملت على بيانات خاصة بالمستخدمين أو المستهلكين. كما أن العولمة تجعل التجسس التجاري الرقمي طريقة أكثر خصوبة بالنسبة للدول. فمع سعي الشركات إلى التوسع والوصول إلى أسواق جديدة، يمكن للمعلومات الداخلية حول عملياتها وخططها المستقبلية أن تساعد الكيانات المحلية على الفوز بعقود وتحقيق التعاطف الإقليمي معها. ولكي نرى مدى صحة ذلك، وما يعنيه في المستقبل، علينا أن ننظر إلى الصين مرة أخرى.

فمع أن الصين ليست بأي حال من الأحوال البلد الوحيد المتورط في هجمات سايبرية على شركات أجنبية، إلاّ أنها أكثر هذه الدول تعقيداً وتحقيقاً للنجاح. فاستعداد بكين للانخراط في التجسس التجاري، ولفرض ذلك على شركاتها، يزيد الشركات الأجنبية ضعفاً، ليس فقط تلك التي تتطلع إلى العمل في الصين، بل جميع الشركات في العالم. فمن الصعب اعتبار الهجوم السايبري الصيني المذكور آنفاً على غوغل والعشرات من الشركات الأخرى عام 2009 حالة معزولة، ففي السنوات القليلة المنصرمة فقط، استهدفت حملات التجسس الصناعي التي قادتها وكالات الجاسوسية الصينية شركات أمريكية تنتج كل شيء، من أنصاف النواقل، إلى المركبات ذات المحركات، فتقانة الدفع النفثي (وليس التجسس التجاري بالظاهرة الجديدة بالطبع، ففي مثال شهير من القرن التاسع عشر كلفت شركة الهند الشرقية التابعة لإنكلترا عالم نباتات اسكتلنديًّا بتهريب نباتات وأسرار صينية من الصين إلى الهند، الأمر الذي نجح في تحقيقه عندما تخفى في ملابس تاجر صيني، وذلك لكسر الاحتكار الصيني للشاي).

أما الجديد في هذه الحلقة الأخيرة من التجسس التجاري، فهو أن الكثير من العمل يمكن إنجازه عن بعد، ومع إغفال شبه تام للهوية في الحقبة الرقمية. وكما سنرى بعد قليل خلال مناقشتنا للحرب المؤتمتة، فإن هذا التطور التقني الجديد سيكون حاسماً في أثره في كثير من المناطق في عالمنا المستقبلي. فنحن نعيش

في عصر التوسع، والصين وغيرها من القوى العظمى الناشئة تسعى إلى توسيع تواجدها الاقتصادي حول العالم. ومن شأن التجسس التجاري الرقمي أن يحسن قدراتها على النمو تحسيناً كبيراً. وسواء أكان ذلك بتمويل رسمي من الحكومة أم بمجرد تشجيع منها، فإن اختراق البريد الإلكتروني للمنافسين وأنظمتهم للوصول إلى معلومات تجارية، سيتيح للاّعبين بلا شك ميزة تنافسية غير عادلة في السوق. وقد حدثنا العديد من القادة التجاريين للشركات التجارية الكبرى بكل ثقة عن الصفقات التي فقدوها في أفريقيا وفي غيرها من الأسواق الناشئة بسبب ما يعتقدون أنه تجسس سلمي، أو سرقة معلومات حساسة (يتم استخدامها لإفساد صفقاتهم أو الاستيلاء عليها).

تبدو معظم حالات التجسس التجاري بين الصين والولايات المتحدة اليوم وكأنها من صنع أفراد انتهازيين، إذ لا تلحظ فيها بصمات الدولة. فثمة زوجان صينيان قاما بسرقة معلومات تجارية متعلقة بأبحاث جنرال موتورز حول السيارات الهجينة (والتي قدرت الشركة قيمتها بأربعين مليون دولار)، وحاولا بيعها إلى شركة شيري للسيارات؛ المنافس الصيني. وهناك أيضاً موظف صيني من شركة فالسبار، إحدى الشركات الكبرى المصنّعة للطّلاء والكساء الخارجي، قام يتن-زيل معلومات سرية بشكل غير قانوني تصل قيمتها إلى 20 مليون دولار معتزماً بيعها للصين. كما سرق الباحث الكيميائي ديبون معلومات حول الصمامات الإلكترونية البيولوجية المصدّرة للضوء، والتي كان يخطط لإعطائها لجامعة صينية. ولم يكن أحد من هؤلاء على علاقة مباشرة بالحكومة الصينية، بل كانوا بالفعل مجرد أفراد يتطلعون إلى تحقيق الأرباح عبر الاتجار بالأسرار التجارية. لكننا نعلم أيضاً أنّ الحكومة في الصين - حيث معظم الشركات الكبرى إما مملوكة للدولة أو خاضعة لنفوذ الدولة خضوعاً كبيراً - قامت بقيادة الكثير من الهجمات السايبرية الهادفة إلى جمع المعلومات الاستخباراتية ضد شركات أمريكية، أو أجازتها.

ومن الصعب الشك في أن الهجمات التي نعلم بها لا تمثل سوى نسبة ضئيلة من مجموع الهجمات التي شُرع بها، سواء أكتب لها النجاح أم لا. ولن تتخذ الولايات المتحدة المسار نفسه من التجسس التجاري الرقمي لأن قوانينها أكثر صرامة (وأفضل تنفيذاً)، ولأن المنافسة غير المشروعة لا تنسجم مع الحس الأمريكي للعب العادل. وهنا يكمن الفرق في القيم بقدر ما هو فرق قانوني. فكما سبق وناقشنا، لا تعير الصين اليوم حقوق الملكية الفكرية قيمة كبيرة. لكن التفاوت بين الشركات الأمريكية والصينية وتكتيكاتها سيكون جوراً على الحكومة والشركات في الولايات المتحدة في الوقت نفسه؛ حيث سيتوجب على الشركات الأمريكية أن تحمي معلوماتها الخاصة بشراسة وأن تحرس حدود شبكاتها، بالإضافة إلى الاحتراس من طيف واسع من التهديدات الداخلية (فجميع الأفراد المذكورين في الأمثلة السابقة كانوا يعملون بشكل قانوني لدى هذه الشركات)، لمجرد الحفاظ على قدرتها التنافسية.

سيستمر التجسس الاقتصادي الحالي لعقود قادمة. سواء أكان بين الولايات المتحدة والصين أم بين بلدان أخرى تتوصل إلى القدرات التقانية المطلوبة، وتدرك الميزات التنافسية التي تقدمها لها. ولن يكون هناك تصعيد دراماتيكي للسبب نفسه الذي سيشعل حرب شيفرات مستقرة نسبياً، لكن مستمرة؛ أي العجز عن تحديد الفاعل في الهجمات السايبرية. وستبقى الحكومة الصينية حرة في دعمها أو مشاركتها بأي عدد من الهجمات السايبرية ضد شركات أجنبية أو منظمات لحقوق الإنسان طالما بقي تورطها غير قابل للإثبات بشكل قطعي[*].

لكن، ثمة استراتيجيات يمكننا اعتمادها للتخفيف من الأضرار الناجمة عن الهجمات السايبرية، إضافة إلى التوصل إلى نقاط ضعف معينة على جانب المهاجمين. ومن بين هذه الاستراتيجيات ما اقترحه كريغ مندي من مايكروسوفت: الحَجْر الافتراضي. فكما وصفنا سابقاً، يأتي الكثير من الهجمات السايبرية اليوم

على شكل هجمات حجب خدمة موزعة أو عادية. وهي هجمات تتطلب استخدام حاسب "مفتوح" وغير آمن على الشبكة يمكن للمهاجم استخدامه كقاعد لعملياته لبناء "جيش من الزومبيات" يتكون من الأجهزة المخترقة (يمكن أن تتولد هجومات حجب الخدمة عن عدد صغير من الآلات المهاجمة عالية النشاط، لكن الهجمات الموزعة تتولد في شبكة ضخمة موزعة من الآلات المهاجمة، غالباً ما يتم اختراقها من بين حواسب ضحية تعود إلى مستخدمين عاديين، يجهلون حقيقة أن حواسبهم تتعرض للتلاعب على هذا النحو). ويمكن لجهاز مهمل أو غير محمي على الشبكة (كحاسب شخصي لا يتم استخدامه في مخبر علمي، أو حاسب شخصي يحضره موظف معه إلى عمله) أن يصبح قاعدة للمهاجم ينال عبره من النظام برمته*.

تستطيع آليات الحجر احتواء هذا الهجوم عبر تمكين مزود خدمة الإنترنت من إغلاق الحاسب المصاب فور التعرف عليه بقرار من طرف واحد، ومن دون ترخيص من صاحبه، ليخرج الحاسب عن الشبكة. "ترتكز الفكرة الأساسية على إيجاد طريقة لإبطاء معدل الانتشار عندما يتم اكتشاف مرض شبكي"، يشرح مندي، "فنحن نحجر على الناس رغماً عنهم، أما في الفضاء السايبري، فإننا لم نقرر بعد إن كان الحجر هو التصرف الصحيح"، مضيفاً أنه "عندما يظهر في أية آلة فيروس أو مرض، أو تظهر عليها علامات على وجودهما، فلا بد من عزلها واحتوائها وإبرائها قبل وصلها بنظام معافى". وكثيراً ما لا يدرك المستخدمون أن حواسبهم مخترقة، لذا إن السماح لمزودي خدمة الإنترنت بإدارة مثل هذه الإجراءات سيضمن حلولاً أسرع بكثير. ووفقاً لطريقة عمل الآلية المتبعة ونوع الهجوم المستخدم، إما أن يدرك المهاجمون أن الجهاز المصاب مفصول عن الخدمة، أو لن يدركوا ذلك، لكن المستخدم سيجد اتصاله بالإنترنت مقطوعاً بقرار من مزود الخدمة. ومع حرمان المهاجمين من القدرة على الوصول إلى الحاسب المصاب، سيتم الحد إلى درجة كبيرة من الضرر الذي يستطيعون إلحاقه.

ووفقاً لرؤية مندي، ستكون هناك منظمة دولية حيادية يرفع إليها مزودو خدمة الإنترنت عناوين الإنترنت التابعة للحواسب المصابة، وبهذه الطريقة يمكن لمزودي خدمة الإنترنت وللدول في العالم عدم السماح لعناوين الإنترنت المحجور عليها بالدخول إلى فضائها الشبكي؛ مما يحد من مجال الهجوم السايبري. وفي هذه الأثناء، يمكن للمحققين مراقبة المهاجمين السايبريين عن بعد (حيث لن يكون المهاجمون على علم بأن الجهاز قد تم الحجر عليه) وجمع المعلومات عنهم؛ بما يساعد على تتبع مصدر الهجمات. أما المستخدم، فلن يخرج عنوان الإنترنت الخاص به من الحجر إلى أن يثبت أنه قام بتنظيف جهازه (باستخدام برمجيات خاصة لمكافحة الفيروسات). وإضافة إلى المنظمة الدولية التي تقود هذه التغييرات، قد نشهد على التوازي إبرام معاهدة دولية تتناول آلية الفصل الآلي. وستمثِّل المعاهدة الدولية للتصرف الفوري في التعامل مع الشبكات المصابة خطوة هامة لمكافحة الهجمات السايبرية. أما الدول التي لا توافق على المعاهدة، فقد تغامر بجعل بلدانها محجورة بكاملها، فتُفصل عن الشبكة، وتحجب عن الكثير من المستخدمين في العالم.

إذا توفر أمن شبكي أقوى فستتاح للأهداف المحتملة فرص أكبر قبل أن يصبح الحجر ضرورياً بوقت طويل. فمن المشاكل الأساسية في أمن الحواسب أن بناء الدفاعات يتطلب من الجهد قدراً أكبر بكثير من الاختراقات نفسها في العادة، حيث تتطلب برامج حماية المعلومات الحساسة أحياناً ما يصل إلى 10 ملايين سطر من الشيفرة البرمجية، بينما يستطيع المهاجمون اختراقها بنحو 125 سطراً فقط. وقد وضحت لنا ريجينا دوغان، نائب رئيس غوغل والمديرة السابقة في داربا (وكالة مشاريع أبحاث الدفاع المتقدمة) التي كانت تتولى فيها مهاماً تشتمل على تطوير الأمن السايبري لصالح حكومة الولايات المتحدة، كيف عملوا على مواجهة هذا الخلل في التوازن على نحو فعال عبر "اختيار التغييرات التقانية التي من شأنها تغيير هذا الخلل الأساسي". ولجأت دوغان وداربا، على غرار مندي، إلى البيولوجيا كطريقة لمواجهة هذا الخلل. فجُمع خبراء في الأمن السايبري مع علماء في الأمراض المعدية، وكانت النتيجة برنامجاً يدعى كراش، أو تصميم الحجر النظيف للمضيفين المرنين المتأقلمين الآمنين.

وتقوم الفلسفة التي بني عليها هذا البرنامج على ملاحظة التنوع الجيني الذي تتمتع به الأجساد البشرية التي تمتلك نظماً مناعية مصممة لمعالجة الفيروسات التي تمر بها والتأقلم معها. تميل الحواسب إلى التشابه في بنيتها، مما يمكن البرمجيات الخبيثة من مهاجمة عدد كبير من الأنظمة بفعالية. "ما لاحظناه في الأمن السايبري"، تقول دوغان،"هو أننا بحاجة إلى ابتكار مكافئ لنظام المناعة المتكيف ضمن العمارة الأمنية الحاسوبية". ويمكن للحواسب أن تبقى متشابهة في مظهرها وطريقة عملها، لكن لا بد من إيجاد فروقات مميزة بينها يتم تطويرها عبر الوقت لحماية كل نظام وتمييزه عن غيره. "وذلك يعني أنه يجب على المهاجم اليوم أن يكتب 125 سطراً من الشيفرة البرمجية لمهاجمة ملايين الحواسب. ومن هنا يتم تعديل هذا الخلل". ولا شك في أن الدرس الذي تم تعلمه قابل للتطبيق في ما يتجاوز الأمن السايبري. فكما تقول دوغان: "إذا كنت ترى في هذه المشاهدة الأولية أنك في موقع خاسر، فعليك أن تقوم بشيء مختلف كلياً، وهذا بحد ذاته كفيل بإيجاد مخارج للمشكلة". أي بعبارة أخرى، إذا كنت غير قادر على ربح اللعبة، فعليك أن تغيّر القواعد.

لكن، على الرغم من توفر بعض الأدوات للتعامل مع الهجمات السايبرية، سيبقى العجز عن تحديد الفاعل على الإنترنت تحدياً جدياً يواجه أمن الحواسب والشبكات. حيث يستحيل بشكل عام - مع تواجد طبقات "لإغفال الهوية" بين كل عقدة وأخرى على الإنترنت - تتبع حزم البيانات للوصول إلى مصدرها. وحين نعالج هذه المسائل، علينا أن نتذكر أن الإنترنت لم يتم بناؤها مع أخذ المجرمين بالاعتبار، بل كانت مبنية على نموذج من الثقة. لذا لا يزال تحديد هوية من تتعامل معه على الشبكة يمثل تحدياً. ومع تحسن قدرات خبراء الأمن في تقانة المعلومات على حماية المستخدمين والأنظمة والمعلومات كل يوم، يزداد في الوقت نفسه تقدم العناصر الإجرامية والفوضوية على الوب. وستستمر لعبة القط والفأر هذه طالما بقيت الإنترنت. وفي النهاية سيساعد نشر تفاصيل البرمجيات الخبيثة والهجمات

السايبرية. فبعد نشر مكونات دودة ستوكسنيت وتفكيكها، تم سد الثغرات في البرمجيات التي تستغلها، وتمكن خبراء الأمن السايبري من العمل على حماية الأنظمة من البرمجيات الخبيثة المشابهة. وقد تنفع استراتيجيات معينة، مثل التسجيل العمومي للمستخدم، لكن طريقاً طويلة لا بد لنا من قطعها قبل أن يصبح لأمن الإنترنت في كل مكان ما يكفي من الفعالية لمنع الهجمات السايبرية البسيطة. ونحن مرة أخرى أمام ازدواجية في العالم الافتراضي، فإغفال الهوية يحمل فرصاً واعدةً للخير كما للشر، سواء أكان الفاعل فرداً مدنياً أم دولة أم شركة، وسيكون الأمر في النهاية منوطاً بالبشر وبطريقة تجسد هذه الفرص في المستقبل.

خلاصة القول، إن الدول ستحن إلى تلك الأيام التي لم يكن عليها فيها سوى التفكير بالسياسات الخارجية والمحلية في العالم الفيزيائي. ولو كان بالإمكان استنساخ هذه السياسات إلى المملكة الافتراضية فلربما كان مستقبل فن السياسة أقل تعقيداً. لكن، على الدول أن تتعايش مع حقيقة أن الحكم في الوطن مع فرض النفوذ في الخارج بات أصعب بكثير اليوم. وستستخدم الدول الأدوات الأكثر فعالية المتوافرة بين أيديها - ومن بينها السيطرة التي تتمتع بها على الإنترنت في بلدانها - لتغير التجربة التي يعيشها مواطنوها على الإنترنت، وستتعاون مع حلفاء يشبهونها في عقلياتهم لممارسة النفوذ في العالم الافتراضي. والتباين في القوة بين العالم الحقيقي والعالم الافتراضي يتيح فرصاً جديدة أمام فاعلين جدد غير متوقعين؛ كالدول الصغيرة التي تسعى إلى القفز متجاوزة وزنها، أو مشاريع الدول التي تتمتع بما يكفي من الشجاعة.

والدول التي تطمح إلى فهم سلوك الدول الأخرى، والأكاديميات التي تدرس العلاقات الدولية، والمنظمات غير الحكومية، والأعمال التجارية العاملة على الأرض ضمن منطقة ذات سيادة؛ ستحتاج كلها إلى تقديرات منفصلة بين العالمين المادي والافتراضي، لذا عليها أن تفهم ما هي الأحداث التي تحدث في أحد العالمين وتؤثر في كليهما، وأن تعرف كيف تتحرك في ظل التناقضات التي قد تتواجد بين السياسات الخارجية والمحلية للحكومة، الفيزيائية منها والافتراضية؛ وهي كلها مهام ينطوي تنفيذها الصحيح على قدر من الصعوبة في العالم الفيزيائي وحده. أما في العصر الرقمي، فسيحدث قدر أكبر من الأخطاء وإساءة الحسابات، وستكون النتيجة على المستوى الدولي المزيد من الصراعات السايبرية وأنواعاً جديدة من الحروب الفيزيائية، وكما سنرى بعد قليل، ثورات جديدة.

الفصل الرابع

مستقبل الثورة

جميعنا نعرف الربيع العربـي، لكن ما نجهله هو ما سيتبعه. فما من شك في أن المستقبل القريب سيكون مليئاً بالحركات الثورية بعد أن تسمح تقانات الاتصالات

ببناء روابط جديدة وتفسح مزيداً من المجال للتعبير. ومن الواضح أن أنشطة تكتيكية معينة، كتعبئة الجماهير أو نشر المواد، ستصبح أسهل مع ارتفاع معدلات انتشار الإنترنت والهواتف الخلوية في الكثير من البلدان.

لكننا على الرغم من ظهور المزيد من الحركات الثورية، سنشهد قدراً أقل من النتائج الثورية، أي عدداً أقل من الثورات التي ستنتهي مسيرتها بتحولات سياسية تقدمية جذرية. وسيعيق غياب القادة القادرين على الاستمرار، إضافة إلى الاستجابات الحكيمة من قبل الدولة، حدوث تغيير عميق (سواء أكان هذا التغيير جيداً أم سيئاً) من مستوى الثورات العربية التي بدأت في نهاية عام 2010. فلطالما حفزت تقانات العصر الثورات وحددت مسيرتها عبر التاريخ. لكن جميع الثورات الناجحة كانت لها في أساسها عوامل مشتركة؛ كالبنية المؤسساتية والدعم الخارجي والانسجام الثقافي. والسجلات التاريخية حافلة بالمحاولات الفاشلة التي كانت تفتقر إلى هذه العناصر؛ من المحاولات الثورية في روسيا التي سبقت عام 1917، إلى الانتفاضة الشيعية في العراق عام 1991، والثورة الخضراء في إيران عام 2. والتقانات الحديثة - على الرغم من قوتها - لا تستطيع أن تصنع الأعاجيب؛ وإن كان بإمكانها تحسين فرص النجاح تحسيناً هائلاً.

فوجود كل هذا العدد من الناس المتصلين والموزعين على أماكن كثيرة يبشر بأن المستقبل سيكشف عن المجتمع المدني الأكثر نشاطاً وتعبيراً وعولمة على الإطلاق. ففي بداية الحركات الثورية، ستقف الطبيعة الضوضائية للعالم حجر عثرة أمام قدرة أمن الدولة على مواكبة الفعالية الثورية وسحقها؛ مما سيمكن الثورة من الانطلاق. لكن السرعة التي يمكن أن يحدث بها ذلك تمثل مشكلة جديدة؛ لأنّه يجب على القادة عندئذ أن يعملوا عبر العالم المادي المكون من برلمانات ودساتير وسياسات انتخابية، ولن يكون لديهم ما يكفي من المهارة والخبرة لتوجيه أي منها على نحو فعال.

البداية أسهل...

مع انتشار إمكانيات الاتصال والاستقبال في مناطق جديدة من العالم في الحظيرة الشبكية، سيستمر إنبات الثورة. وسيكون ذلك أكثر عفوية وأشد تواتراً من أي وقت مضى في التاريخ. فمع توفر الفضاء الافتراضي على هذا النحو الجديد بما يحمله من تقانات، ستغتنم الشعوب والمجموعات في جميع أنحاء العالم هذه الفرصة لتعرض بإيمان وثبات مظالم كظمتها طويلاً أو مشكلات جديدة تهمها. وسيكون كثيرون ممن سيتحملون هذه المسؤوليات شباباً؛ ليس فقط لأن الكثير من البلدان القادمة إلى الشبكة تتكون من أمم فتية على نحو لا يصدق (ولنا في أثيوبيا وباكستان والفلبين ثلاثة أمثلة لبلدان معظم سكانها لم يتجاوزوا الخامسة والثلاثين)، بل أيضاً لأن اجتماع النشاط بالنـزق عند الشباب ظاهرة عامة. فالشباب يعتقدون مسبقاً أنهم قادرون على إصلاح الأشياء، لذا لن يترددوا إذا سنحت لهم الفرصة.

ستعيش جميع المجتمعات في المستقبل - بما فيها تلك التي تبنت تقانة الإنترنت

في وقتٍ مبكر - أشكالاً مختلفة من الاحتجاج، تُستخدم فيها تقانات الاتصال لأغراض التنظيم والتعبئة ولمخاطبة المجتمع الدولي. وستتحول المنصات التي يستخدمها المحتجون اليوم (كالفيسبوك وتويتر ويوتيوب وغيرها) إلى وسائط أكثر فائدةً مع إيجاد المطورين حول العالم طرقاً جديدة يستغلون فيها الفيديوهات والصور والرسائل المرتبطة بمهام بعينها. وسيشهد العالم نشطاء أكثر رقميةً يعتبرهم المجتمع الدولي أبطالاً، ويسعون لأن يصبحوا سفراء لقضاياهم. أما البلدان التي لم تشهد الاحتجاجات الأولى الكبرى في العصر الرقمي حتى الآن، فستعيشها على نطاقٍ عالمي حين يكون العالم كله مراقباً لها، حتى إنه قد يبالغ في تقدير أهمية ما يحدث. وستشهد المجتمعات الديموقراطية مزيداً من الاحتجاجات المتعلقة بالمظالم الاجتماعية والتباينات الاقتصادية الملموسة، بينما سيتظاهر الناس في البلدان القمعية احتجاجاً على مواضيع مثل تزوير الانتخابات والفساد ووحشية الشرطة. وستكون قليلة تلك القضايا الجديدة حقاً، لكن ما سيتغير هو أشكال التعبئة التي ستتحسن وأعداد المشاركين التي ستتزايد إلى حدّ كبير.

لطالما كان تنفيذ ثورة محصوراً بفئة من الأفراد الذين يحملون الأسلحة الصحيحة، ويتمتعون بالدعم الدولي أو التدريب. لكن جزءاً كبيراً من هذا الاحتكار شرع بالتفتت مع انهيار الحواجز المتعلقة بالعمر والجنس والظروف والحالة الاقتصادية الاجتماعية التي كانت تمنع الأفراد من المشاركة في السابق تحت وطأة تقانات الاتصالات. فلن يعاني المواطنون بعد اليوم من الظلم في عزلةٍ ووحدة، وستكون حلقة التغذية الراجعة المعولمة هذه، والتي يمكن من خلالها للناس حول العالم التعليق وإظهار ردود الأفعال، إلهاماً للكثير من الشعوب يدفعها إلى النهوض والتعبير عن مشاعرها. وكما بيّنت ثورات الربيع العربـي، ما إن يحطم ما يدعى حاجز الخوف، ويظهر الضعف على الحكومة بطريقةٍ جديدة، حتى يكفّ المواطنون - الذين كانوا لولا ذلك منصاعين وهادئين - عن ترددهم وينضموا إلى الركب. وقد كانت إحدى التبعات الإيجابية للوسائط الاجتماعية خلال الثورات العربية على سبيل المثال تمكّن النساء من لعب دورٍ أعظم بكثير؛ حيث كان لديهنّ خيار التعبير عن أنفسهن عبر الشبكات الاجتماعية حين كان الخروج إلى الشوارع مجازفةً (وإن كانت بعض النساء قد قبلن بالمجازفة المادية بالفعل). ففي بعض البلدان، سيقوم الناس بتنظيم الاحتجاجات على الشبكة، أو في الشارع كل يوم أحياناً؛ لأنهم ببساطة قادرون على ذلك. وقد رأينا ذلك عندما زرنا ليبيا عام 2012، فعندما قابلنا الوزراء في الحكومة الانتقالية في طرابلس ذكروا لنا عفوياً أن هنالك مجموعاتٍ صغيرة من المحتجين يخرجون كل صباحٍ تقريباً. فهل كان ذلك يقلقهم؟ سألناهم، كان ذلك يقلق بعضهم، لكن الآخرين هزوا رؤوسهم وهم يكادون يضحكون قائلين إنه رد فعلٍ طبيعي بعد أكثر من أربعين عاماً من القمع.

يفسح المجال الافتراضي مساحاتٍ جديدةً للاعتراض والمشاركة، كما يقدم حماياتٍ جديدة للثوريين المحتملين. إذ سيجد المعارضون العالم أكثر أماناً في معظم الحالات بفضل الانتشار الواسع لتقانات الاتصالات، وإن كانت المخاطر الفيزيائية التي يواجهونها لن تتغير (كما أن الاتصالات لن تحمي جميع الناشطين

بالقدر نفسه. ففي البلدان التي تتمتع حكوماتها بقدرةٍ تقانيةٍ عالية، سيشعر المعارضون بالضعف على الشبكة؛ تماماً كما يشعرون به في الشوارع). فالاعتقالات والانتهاكات والتعذيب والاغتيالات لن تختفي. لكن إغفال الهوية على الإنترنت، والقوة الشبكية لتقانات الاتصالات سيؤمّنان للناشطين في كل مكان، وللمشاركين المحتملين، طبقةً جديدة من العزل الوقائي ستشجعهم على المتابعة.

ستكون تطورات تقنية معينة عوناً كبيراً للناشطين والمعارضين. فبرمجيات الترجمة الفورية الدقيقة ستمكنهم من مشاركة المعلومات وراء الحدود. وسيساعد الوصول الإلكتروني الموثوق إلى معلوماتٍ خارجية وإلى الجاليات في المغترب على مواجهة روايات الدولة التي قد تكون مضللة، وعلى زيادة حجم قاعدة الدعم زيادةً واضحة. وستساهم المنصات الإلكترونية الآمنة التي تساعد على نقل الأموال أو تبادل المعلومات في دعم تواصل المحتجين مع مصادر الدعم الخارجية من دون إثارة الشبهات حول موقعهم الحقيقي.

ستشتمل الحركات الثورية الجديدة على عدد من الناشطين مجهولي الهوية الذين ينشطون بدوام جزئي أكبر مما نشهده في حركات اليوم. وذلك ببساطة لأن المواطنين سيتمتعون بمزيد من السيطرة على توقيت تمردهم وكيفيّته. فقد كان النشاط الثوري ذات يوم يستلزم التزاماً شخصياً تاماً. أما اليوم، وأكثر بعد في المستقبل، فستسمح المنصات التقانية متعددة المظاهر للبعض بالمشاركة بدوام كامل، بينما يساهم آخرون بما يستطيعون المساهمة به خلال استراحة الغداء. وسيستفيد الناشطون في المستقبل من المعرفة الجمعية للأشخاص والناشطين الآخرين في العالم؛ وخصوصاً في ما يتعلق بحماية أنفسهم. فالبروتوكولات الأمنية وأدوات التشفير وغيرها من أشكال الأمن الإلكتروني ستتوفر على نطاق أوسع، وسيتحسن فهم الناس لها. سيكون معظم القادمين الجدد إلى الإنترنت خلال العقد القادم خاضعين لحكومات شبه مستبدة. والتاريخ يقول إن الحفاظ على الحكومات الدينية وثقافات عبادة الفرد والديكتاتوريات يكون أصعب بكثير في حقبة يتعاظم فيها انتشار المعلومات. وليس بوسع المرء سوى أن يفكر بالدور الذي لعبته سياسة المكاشفة ("الانفتاح") في انهيار الاتحاد السوفييتي. وفي النهاية، سنشهد في أنحاء العالم ظهور نماذج لشعوب أتيح لها الوصول إلى الفضاء الافتراضي وإلى المعلومات الجديدة، تتمرد باستمرار ضد حكوماتها القمعية أو غير الشفافة على الشبكة؛ إلى حد يجعل أمارات الثورة حالة دائمةً بالفعل.

سيغير انتشار الاتصالات من نظرتنا إلى المجموعات المعارضة في المستقبل. فالمنظمات والأحزاب المادية ستبقى عاملة داخل البلدان، لكن وفرة المشاركين في الميدان الافتراضي ستغير مشهد النشطاء تغييراً جذرياً. ولن يربط الناس أنفسهم بقضية واحدة، بل سينضمون عوضاً عن ذلك إلى حركات منتشرة عبر بلدان متعددة تتبنى مواضيع مختلفة. وسيساعد هذا التوجه منظمي الحملات ويثبط هممهم في آن معاً، حيث سيكون من الأسهل تقدير شبكة داعميهم وتخيلها، لكن سيصعب تقدير مدى التزام كل مشارك ومدى اهتمامه. ففي البلدان التي تكون فيها حرية الاجتماع محدودة أو غائبة، ستكون فرصة التواصل والتخطيط في الفضاء

الافتراضي هبة من الله، بغض النظر عن هوية المشاركين. لكن القرار الاستراتيجي المتعلق بجعل حركة ما مدعومة من الجماهير بالفعل أو مجرد غرفة صدى كبيرة سيكون بشكل عام منوطاً بأولئك الذين يحتلون مواقع قيادية فيها.

يقدم العالم الشبكي للمجموعات المعارضة إمكانيات جديدة لإنجاز مهام حيوية كجمع التبرعات وبناء الاسم. فقد تختار المنظمات تمثيل نفسها بطريقة مختلفة في الزوايا المختلفة على الإنترنت للوصول إلى شرائح سكانية مختلفة، حيث تخفف مجموعة مقاوِمة في وسط آسيا نبرتها الدينية، وتسوِّق لمواقفها التحررية عندما تكون على منصات ناطقة بالإنكليزية يسودها مستخدمون غربيون، بينما تقوم بالنقيض على الشبكات التابعة لمنطقتها. ولا يختلف ذلك عما يقوم به الإخوان المسلمون وأحزابهم الإسلامية اليوم، أو ما تبديه الجزيرة بنسختيها العربية والإنكليزية من اختلاف في اللهجة والتغطية. (ففي أحد أيام الاحتجاجات المنوي تنظيمها في مرحلة مبكرة من الثورة السورية عام 2011 على سبيل المثال، سارعت الجزيرة الإنكليزية إلى إيراد عدد الوفيات بين المحتجين، بينما لم يرد الرقم على موقع الجزيرة العربية الذي ركز بدلاً عن ذلك على انفتاح ضئيل أبداه بشار الأسد تجاه الأقلية الكردية في البلاد. ويرى بعض المحللين أن هذا التفاوت يعود إلى التباين السياسي للمحطة العربية إزاء إيران؛ حليفة سوريا وجارة قطر حيث مقر الجزيرة).

بينما تتنامى الفرص المتاحة أمام هذه المجموعات لبناء اسمها، سيتغير النموذج القديم للمنظمة المعارضة. إذ تمتلك المجموعات اليوم مواقع وب بدلاً من المكاتب، وتمتلك متابعين وأعضاء بدلاً من الكوادر. وهي تستخدم منصاتٍ مجانية متوفرة للعموم تحررها من الكثير من التكاليف الثابتة، وسيكون هناك العديد من الجبهات الرقمية كهذه في المستقبل مما يجعل المنافسة على جذب اهتمام الجماهير بين المجموعات في العالم على أشدها.

وسيؤدي تكاثر الأصوات الجديدة على الشبكة والجلبة التي تصدرها إلى ضرورة أن نقوم جميعاً بتعديل تعريفنا للمعارضين. ففي النهاية، ليس كل من يتكلم ويعبر عن رأيه على الإنترنت (وهو ما ينطبق على الجميع تقريباً أو على كل من يمتلك اتصال إنترنت) معارضاً. أما الذين سيطفون على السطح خلال الموجة القادمة من القادة المعارضين فسيكونون أولئك الذين يستطيعون توجيه متابعيهم، وحشد جمهورهم لدعمهم على الشبكة، ومن يمتلكون قدراتٍ واضحة في استخدام أدوات التسويق الرقمية، والمستعدين - وهذا هو الأهم - للمخاطرة بسلامتهم. فالنشاط الرقمي - خصوصاً إذا تم عن بعد ومع إغفال الهوية - يخفف من الرهان الذي يجب على الراغبين في ممارسة المعارضة وضعه. لذا، سيتميز القادة الحقيقيون باتخاذهم مجازفات مادية لا يستطيع داعموهم الافتراضيون اتخاذها أو لا يرغبون في القيام بها. ومن المرجح أن يجد أولئك الذين يتمتعون بمعرفةٍ عميقة بالإصلاح الدستوري وبناء المؤسسات ومواضيع الحكم، لكن تنقصهم المعرفة التقنية المتوفرة لدى الناشطين الآخرين، أنفسهم عرضةً لخطر التخلف عن الركب؛ حيث سيجدون صعوبة في البروز بين الجماهير الافتراضية، وفي إثبات قيمتهم أمام

القادة الشباب الجدد (الذين قد لا يستوعبون الصلة الحقيقية لتجاربهم بما يجري).

ستكون الحركات الثورية في المستقبل - كما قلنا - عابرةً للقوميات، وشاملةً أكثر من الكثير (لكن ليس من جميع) من الثورات السابقة؛ حيث ستمتد خارج الحدود التقليدية للقومية والإثنية والعرق والجنس والدين. فخلال رحلةٍ إلى تونس عام 2011، قابلنا ناشطين من ثورة الياسمين قبيل الذكرى السنوية الأولى لثورتهم الناجحة. وعندما سألنا عن السبب الذي جعل ثورتهم تطلق شرارة سلسلةٍ من الثورات الأخرى في تتابعٍ سريع اعترفوا بوجود مظالم مشتركة، لكنهم أشاروا بعدها إلى شبكاتهم الإقليمية، حيث كان باستطاعتهم بناء العلاقات مع الغرباء ممن يتحدثون العربية ويعيشون في الشرق الأوسط بسرعة كما يقولون. وذلك ليس بفضل اللغة والثقافة المشتركتين فقط، بل لأنه كان لديهم أصدقاء مشتركون أيضاً. أي إن الاتصالات الاجتماعية الموسعة والموجودة مسبقاً تم تفعيلها وتنشيطها مع اجتياح الروح الثورية للمنطقة؛ الأمر الذي نتج عنه تبادل الاستراتيجيات والأدوات والأموال والدعم الأخلاقي.

لكن هذه الشبكات الضخمة كانت حدودها محصورة بالعالم العربـي تقريباً. غير أن ذلك لن يكون قائماً في المستقبل، فبرمجيات الترجمة المتقدمة التي تستطيع معالجة اللهجات الإقليمية، والتي تقوم بعملها بشكلٍ متزامن، ستمكن الناشط الناطق بالعربية في المغرب من التنسيق بزمنٍ حقيقي مع ناشطٍ في بانكوك لا يتحدث سوى التايلندية. ومن شأن الترجمة الصوتية المبتكرة، والواجهات الإيمائية الدفقية، وأجهزة الإسقاط الهولوغرافية أن تفتح بوابات الفيض لتتشكل شبكات افتراضية أوسع بكثير مما يتوفر اليوم لأيٍّ كان. ثمة عددٌ لا يحصى من التشابهات الثقافية التي لم يتم استكشافها مطلقاً بسبب صعوبة الاتصالات، أما ضمن الظروف الثورية المستقبلية، فستتكفل الاتصالات التي تبدو عشوائيةً بين شعوبٍ متباعدة أو أشخاصٍ متباعدين، بتدفقٍ معرفي يؤدي إلى تعهيد أنواعٍ معينة من الواجبات وتضخيم حجم رسالة الحركة بطريقة جديدة غير متوقعة.

ستسمح تقانات الاتصالات للبعض بالانخراط في النشاطات من دون أية مجازفة، وبقطف ثمار النشاطات من دون بذل عناء كبير. فمن السهل إعادة تغريد شعار معادٍ للحكومة، أو مشاركة مقطع فيديو يظهر عنف الشرطة الوحشي من مسافةٍ آمنة؛ خصوصاً إذا قورن ذلك مع المخاطر التي يعرّض نفسه لها أي شخصٍ يقوم بتصوير الفيديو من مسافة قريبة. فالناس غير المنخرطين في الحركة مباشرةً قد يشعرون بإحساسٍ حقيقي بالقدرة عبر فعل شيءٍ ما أياً يكن. والمنصات الشبكية تمنح هؤلاء طريقةً للتبرع وللإحساس بقيمتهم؛ حتى إذا كان ما يفعلونه مجرد جهدٍ بسيط ليس له أثرٌ كبير على الأرض. أما بالنسبة لأولئك المقيمين في بلدان يكون فيها خطر أن يضبطهم النظام العارف تقنياً احتمالاً قائماً، فإن الشجاعة الافتراضية لا تخلو من المجازفة.

سيكون بإمكان مراهقٍ في شيكاغو أو طوكيو بلا شك المساهمة بطريقة لا يستهان بها في حملة تجري على مستوى العالم. فبعد قطع إمكانيات الاتصال الخارجية في مصر من قبل نظام مبارك لجأ الكثير من المراقبين إلى حساب على

تويتر أطلقه طالب دراسات في العقد الثاني من عمره في لوس أنجلوس، معتبرين الحساب مصدر معلومات ذا مصداقية. أما الطالب، جون سكوت ريلتون، فكان ينشر تحديثات عن مجريات الاحتجاجات يلتقطها أو يجمعها من مصادر مصرية ليس لديها سوى الهواتف الأرضية. وبقي عنوانه على تويتر (أصوات 25 يناير Jan25voices@) قناة معلومات رئيسة للثورة، وذلك على الرغم من عدم كونه صحافياً أو متحدثاً طليقاً باللغة العربية. لكن على الرغم من تمكن سكوت ريلتون من لفت بعض الانتباه الشعبـي إلى تغريداته، فإن ما يمكن لشخصٍ بمثل سيرته أن يحققه في مجال التأثير على الساسة يبقى محدوداً.

وربما يكون المثال الأهم هو أندي كارفن الذي كان عرّاب إحدى أهم قنوات المعلومات في كلٍّ من الثورتين المصرية والليبية. وكان يتابع هذه القناة عشرات الآلاف من المشتركين، وعدد لا يحصى من الصحفيين حول العالم؛ ممن يعلمون أن كارفن نفسه (وهو أحد كبار المحللين الاستراتيجيين في الراديو الوطني العام) يتمتع بالمعايير الصحافية لمراسلٍ محترف، أي إنه لن يغرد أو يعيد تغريدة شيء لا يمكنه التحقق منه. فأصبح كارفن بمثابة فلتر بجسد رجلٍ يقوم بتجميع المصادر ومعالجتها، ويتمتع بتأثيرٍ هائل.

لكن، مهما فعل أندي كارفن أو جون سكوت ريلتون في العالم، فإن العمل الشاق للحركات الثورية كان يتم على الأرض، ومن قبل أشخاصٍ داخل البلاد مستعدين للخروج إلى الشوارع؛ إذ لا يمكنك اقتحام وزارة الداخلية بهاتفٍ نقال.

ستكون الشجاعة الافتراضية مسؤولة عن تحديد طريقة عمل المحتجين أنفسهم، فمنصات الوسائط الاجتماعية العالمية ستمنح الناشطين والمعارضين المحتملين الثقة في قناعاتهم أو في اعتقادهم بوجود جمهورٍ لهم؛ سواء أكان ذلك صحيحاً أم لا. فقد تبالغ منظمةٌ في تقديرها قيمة الدعم الشبكي؛ متجاهلةً بذلك أولوياتها الأخرى الأكثر صعوبةً، والتي قد تعطيها ميزة حقيقية، مثل إقناع رجال إدارة النظام بالانشقاق. فتوفر شبكة افتراضية ضخمة سيشجع بعض المجموعات على القبول بالمجازفة؛ حتى حين يكون التصعيد غير مضمون. وقد تشن قوة معارضة ما، وقد امتلأت ثقة وشجاعة لما رأته في العالم الافتراضي، حملاتٍ طائشة وغير ناضجة؛ وهي النتيجة النهائية التي لا مفر منها لتحطيم آليات السيطرة التقليدية التي تقيد الحركات الثورية. ولا مفر من استمرار هذه النـزعات من الشجاعة الافتراضية - سواء أكانت من قبل المنظمين أم من قبل أطراف خارجية - لبعض الوقت؛ حتى تتعلم المجموعات المعارضة كيف تستغلها على نحوٍ فعال.

في نهاية المطاف، ستؤدي المعرفة الشعبية المتزايدة بالثورات والحملات الجارية حول العالم إلى نهوض ثقافة المساعدين الثوريين، وستكون هناك أنواع كثيرة منهم. فمنهم من سيكون مفيداً، ومنهم من سيكون مشتِّتاً للانتباه، ومنهم من سيكون خطيراً أيضاً. حيث سنرى مهندسين أذكياء يطورون تطبيقات وأدوات أمنية يشاركونها مع المعارضين، وستقوم مواقع جمع الأصوات على الإنترنت باستغلال وزن الجماهير للضغط والمطالبة بأخذ المطالب بعين الاعتبار. ولا شك في أن البعض سيعدّون أجهزة متخصصة سيتمّ تهريبها إلى البلدان التي تشهد حركات

احتجاجية، وستكون عبارة عن أجهزة محملة مسبقاً بتطبيقات مشفرة تسمح للمستخدمين بنشر المعلومات (من نصوصٍ وصورٍ وأفلام فيديو) من دون ترك أي سجل على الهاتف. ومن دون مثل هذا السجل لن يحتوي الهاتف على أي دليل إدانة، وبالتالي سيبقى مغفل الهوية وعديم الفائدة لأية عصابةٍ أمنية قد تجده.

كما سنرى موجة من السياح الثوريين، وهم أولئك الذين يمضون يومهم كاملاً على الإنترنت؛ بحثاً عن احتجاجات شبكية ينضمون إليها، ويساعدون على تضخيمها، لمجرد الإثارة التي تقدمها لهم. وقد يساعد هؤلاء على الحفاظ على الزخم عبر نشر المحتويات، لكنهم سيكونون خارجين عن السيطرة من دون فلترة أو رقابة. وقد تنحرف رواياتهم عن توقعات الناس الذين يجازفون على الأرض. وستكون المهمة الأساسية للقادة الفعالين في المعارضة، والمدركين لما يتطلبه نجاح الثورة بعد، إيجاد طرق لاستغلال المشاركين الجدد مع ممارسة ضبط الجودة وإدارة التوقعات على نحو فعال.

لكن الخاتمة أصعب...

في النهاية، لن يمثل الانتشار السريع للحركات الثورية عبر المجتمعات حديثة العهد بالاتصالات تهديداً كبيراً للحكومات المستقرة؛ كما يتوقع بعض المراقبين. فبالرغم ممّا تستطيع تقانات الاتصالات أن تقدمه للثورات الانقلابية حيث ترجح كفة الميزان لصالح الشعب، ثمة عناصر تغيير حاسمة لا يمكن لهذه الأدوات التأثير فيها؛ وأولها إنتاج قادة طليعيين، أي الأفراد القادرين على الحفاظ على المعارضة في الأوقات العصيبة، وعلى التفاوض مع الحكومة إذا أريد الإصلاح، وعلى الترشح في الانتخابات والفوز بها، وتحقيق ما يتطلع الشعب إليه بعد فرار الدكتاتور. فلا علاقة للتقانة بتمتع الفرد بالصفات التي تخوله لعب دور رجل الدولة.

لقد رأينا في السنوات الأخيرة كيف يمكن لأعدادٍ كبيرة من الشباب المسلحين بما لا يزيد عن بعض الهواتف النقالة أن يشعلوا ثورات تتحدى عقوداً من السلطة والسيطرة، وأن يسرعوا عملية كانت تتطلب تاريخياً سنوات طويلة. وقد غدا واضحاً كيف يمكن لمنصات التقانة أن تلعب دوراً رئيساً في إسقاط الديكتاتوريات إذا أحسن استخدامها. وإذا أخذ بعين الاعتبار الطيف المتنوع من النتائج الممكنة (كالقمع الوحشي، أو تغير النظام، أو الحرب الأهلية، أو التحول إلى الديموقراطية) فمن الواضح أيضاً أن الشعوب، وليس الأدوات التي تستخدمها، هي التي تقوم بالثورات أو توقفها. وستصبح المكونات التقليدية للمجتمع المدني أكثر أهميةً بعد مع تدفق الحشود الشبكية إلى الساحات الافتراضية العامة؛ لأنه على الرغم من الدور الهام والمؤثر الذي سيلعبه الأفراد المنخرطون في الثورة (كالمهندسين الناشطين) فإن كثيرين غيرهم لن يتجاوز دورهم - كما سبق وقلنا - دور المضخم أو منبع الضجيج الذي يرافق الركب.

ستنجب ثورات المستقبل الكثير من المشاهير، لكن هذا الجانب من صناعة الحركة سيؤخر عملية تطوير القيادات الضرورية لإنهاء المهمة. ويمكن للتقانة أن تساعد على إيجاد الأشخاص المتمتعين بمهارات القيادة من مفكرين ومثقفين وغيرهم، لكنها لا تستطيع إنتاجهم أو بكلمات أخرى إنجابهم. كما يمكن للثورات

الشعبية أن تقلب الديكتاتوريات، لكنها لن تكون ناجحةً بعد ذلك إلا إذا امتلكت قوى المعارضة خطة جيدة ونفذتها. وإلا فإن النتيجة ستكون إما إعادة تنصيب النظام البائد، أو التحول من نظامٍ يعمل إلى دولةٍ فاشلة. ففتح صفحة على الفيسبوك لا يعني تشكيل خطة، لأن المهارات التشغيلية الفعلية هي التي ستحمل الثورة وتضمن لها حسن العاقبة.

وصف الربيع العربـي من قبل مراقبين ومشاركين فيه في آنٍ معاً بأنه "بلا قائد"، لكن ذلك ليس دقيقاً تماماً. فصحيحٌ أنه من الممكن تماماً خلال عملية التظاهر اليومية الحفاظ على بنية قيادة غير مركزية (وهذا أكثر أمناً أيضاً بما أن النظام لا يستطيع القضاء على الحركة ببساطة عبر اعتقال قادتها)، لكن مع الوقت لا بد من ظهورِ شكلٍ من أشكال السلطة المركزية في الحركة؛ إذا أرادت الحركة أن تتخذ اتجاهاً معيناً. فالثوار المقاتلون الذين واجهوا معمر القذافي بجسارة على مدى شهور، لم يكونوا جيشاً متجانساً، لكنهم في 27 شباط عام 2011، أي بعد مضي أسبوعين على الاحتجاجات الشعبية الأولى في ليبيا، قاموا بتشكيل المجلس الانتقالي الوطني في بنغازي. وكانت الهيئة التنفيذية للمجلس - والمكونة من شخصيات معارضة بارزة، ومنشقين عن النظام، ومسؤولين سابقين في الجيش، وأكاديميين، ومحامين، وسياسيين، وكبار رجال الأعمال - بمثابة حكومة معارضة، وكانت تجري التفاوضات مع البلدان الأجنبية ومسؤولي الناتو خلال المعارك ضد القذافي. وبقي رئيس المجلس محمود جبريل رئيس وزراء مؤقّتاً للبلاد حتى تشرين الأول عام 2011؛ أي بعد فترة وجيزة من إلقاء القبض على القذافي وقتله.

أما في تونس، فقد حدثت الثورة بسرعة، ولم تسمح بتشكيل حكومةٍ معارضة على غرار المجلس الانتقالي الوطني الليبـي. وعندما فر الرئيس زين الدين بن علي كانت الدولة التونسية كبنية لا تزال موجودة، وواظب المواطنون على الاحتجاج ضد الحكومة؛ إلى أن استقال من تبقى من أعضاء حزب زين الدين بن علي، التجمع الدستوري الوطني، وشُكلت حكومة مؤقتة اعتبرتها الجماهير مناسبة. ولو أن مسؤولي الحكومة تقاعسوا عن الاستجابة لمطالب الشعب، أو لجأوا إلى اتخاذ إجراءاتٍ صارمة بدلاً من إعادة توزيع المناصب، فلربما اتخذت تونس مساراً مختلفاً جداً يكون أكثر اضطراباً (ومن الجدير بالذكر أن كثيراً من القادة الذين تم انتخابهم في تشرين الأول عام 2011 في الانتخابات التونسية كانوا سجناء سياسيين سابقين يتمتعون بمستوى مختلف - وربما شخصي - من المصداقية لدى الشعب مقارنةً بالعائدين من المنفى). وقد أخبرنا رئيس الوزراء التونسي حمادي الجبالي (وهو نفسه سجين سياسي سابق) أنه يرى أنه يجب على وزير الداخلية الأول الذي يأتي بعد نظام بن علي أن يكون "أحد ضحايا وزارة الداخلية". وهكذا، قام بتعيين علي العريضي لهذا المنصب؛ حيث كان الأخير قد أمضى أربعة عشر عاماً في السجن في ظل النظام السابق، قضى معظمها في زنـزانة انفرادية.

على أنّ سيئة تسريع وتيرة الحركة هو أن فترة الحمل المتاحة للمنظمات وأفكارها واستراتيجياتها وقياداتها تكون أقصر بكثير. وقد برهن التاريخ أن الحركات المعارضة تحتاج إلى الوقت لكي تتطور، وأن الضوابط والتوازنات التي تشكل

الحركة الناشئة تؤدي في نهاية المطاف إلى تقويتها وزيادة قدرتها، وإلى تحقيق تناغمٍ أكبر بين القادة والشعب الذي يريد القادة إلهامه. ولنأخذ هنا الكونغرس الوطني الأفريقي في جنوب أفريقيا مثالاً، فخلال العقود التي أمضتها في المنفى في أثناء فترة الحكم العنصري الأبارتايد، مرت المنظمة بمراحل صقل متعددة منحت الأفراد الذين سيصبحون رؤساء لجنوب أفريقيا (نيلسون مانديلا، وتابو إيمبيكي، وجاكو بزوما) ما يكفي من الوقت لبناء سمعةٍ لهم، ولتحقيق المصداقية وبناء الشبكات، ولشحذ قدراتهم العملياتية في الوقت نفسه. ومثل ذلك ينطبق على ليخ فاونسا واتحاده النقابـي في بولندا، فقد انقضى عقدٌ من الزمن قبل أن يتمكن قادة الاتحاد من خوض غمار الانتخابات البرلمانية ليفتح فوزهم الطريق نحو إسقاط الشيوعية.

تمضي معظم المجموعات المعارضة سنوات في تنظيم القادة وتفعيلهم وتنمية علاقاتهم. وقد سألنا وزير الخارجية السابق هنري كسنجر، الذي التقى جميع القادة الثوريين الكبار المعروفين تقريباً خلال السنوات الأربعين المنصرمة، عما ينقص إذا تم تعجيل هذه الخطوات فقال: "من الصعب تصور شخصيات مؤثرة على غرار ديغول وتشرشل في عالم الفيسبوك"، ففي عصر الاتصالات الفائقة السرعة "لا أرى أفراداً مستعدين لاتخاذ موقفٍ مستقل، أو يمتلكون الثقة الكافية للمواجهة فرادى". فبدلاً من ذلك يوجد نوعٌ من   الذي يدفع العالم، وقلةٌ هم الذين سيكونون مستعدين لمجابهته. وهنا تماماً تكمن المجازفة التي يقبل بها القائد، "فالقيادة المتميزة مسألةٌ إنسانية، ولا يمكن إنتاجها عبر وسط اجتماعي جماهيري" يقول كسنجر.

وفي غياب رجال الدولة والقادة لن يكون هنالك ما يكفي من الأفراد المؤهلين لدفع البلاد قدماً ولتحمل مخاطر استبدال شكل سلطوي بآخر، "فالمواطن المتمكن"، يقول كسنجر، "يعرف تقنية دفع الناس إلى الساحة، لكنه لا يعرف ما عليه فعله معهم حين يصبحون في الساحة. بل وتقل حيلته أكثر بعد أن يكتب لهم النصر". ويتابع موضّحاً: "من السهل تهميش مثل هؤلاء؛ لأن استراتيجياتهم تفقد فعاليتها مع الوقت. إذ لا يمكنك أن تخرج الناس إلى الساحات عشرين مرةً في العام، فثمة حدّ موضوعي. وما من مرحلةٍ تاليةٍ واضحة". وحين لا تكون المرحلة التالية واضحة لا يبقى للحركة ما يدفعها سوى زخمها الداخلي الذي لا بد أنّه سينفد.

ثمة ناشطون في الشارع، ممن لا يتوانون عن انتقاد ثوراتهم ونتائجها، قد يخالفون كسنجر الرأي. وأحد هؤلاء هو محمد سالم، المدون المصري الذي تحول إلى ناشط، وأصبح أشبه بالناطق باسم ثورة بلاده عام 2011. وسالم شديد الانتقاد لرفاقه المصريين نتيجة ما يراه لديهم من عجزٍ على تجاوز الأهداف قصيرة المدى المتمثلة بإسقاط مبارك وفتح النظام السياسي للمنافسة. لكن هذا الانتقاد يخصّ مصر، وليس النموذج الثوري للعصر الرقمي الجديد. فكما كتب في شهر حزيران من عام 2012 بُعيد أول انتخابات رئاسية بعد الثورة في مصر "إذا كنتم ثواراً فأرونا قدراتكم. ابدأوا بشيءٍ ما، انضموا إلى حزب أو أسسوا منظمة. قوموا بحلّ مشكلةٍ حقيقية، افعلوا شيئاً آخر غير التنقل بين المظاهرات والاعتصامات، فهذا ليس عملاً

ميدانياَ. العمل الميداني يعني تحريك الشارع وليس التحرك في الشارع. العمل الميداني الحقيقي يعني أن الشارع الذي تعيش فيه يعرفك ويثق بك وسيتحرك معك". إنه ينصح الناشطين الميدانيين بالمشاركة في الحكم وفي إصلاح ثقافة الفساد التي يناهضونها. وهذا يعني وضع أحزمة الأمان، واحترام قوانين السير، والانضمام إلى أكاديمية الشرطة، والترشح للبرلمان، ومحاسبة المسؤولين المحليين على تصرفاتهم.

يعرض كتاب **الانضمام إلى النادي: كيف يمكن لضغط الأنداد أن يغير العالم** لتينا روزنبرغ، دفاعاً آخر عما يمكن للجماهير إنجازه. فلدى استعراضها أهمية العلاقات الإنسانية في تحديد سلوك الأفراد وفي صياغة التوجهات الاجتماعية الكبرى، تقول الكاتبة إن الثوريين قادرون على توجيه ضغط الأنداد لدفع الأفراد والجماعات إلى سلوكيات أفضل. وربما كان الدليل الأكثر إقناعاً لما تصفه

متجسداً في المجموعة الصربية الناشطة أوتبور التي لعبت دوراً رئيساً في إنهاء نظام سلوبودان ميلوزوفيتش. إذ توضح الكاتبة كيف استخدمت المجموعة حيلاً سريعة؛ كمسرح الشارع، والمقالب، والموسيقى، والصراخ بالشعارات، والعصيان المدني السلمي لكسر ثقافة الخوف واليأس. وحين عمد النظام إلى القضاء على المجموعة كشف عن وجهه الوحشي، والأحمق أحياناً؛ مما زاد من الدعم الذي تتمتع به المجموعة.

لكن الأهم مما تمثله مجموعات مثل أوبتور بالنسبة إلى الماضي هو الدور الذي يمكن لقادتها أن يلعبوه في المستقبل. فكما تشير روزنبرغ في معرض قصة مؤثرة عن ناشطين صربيين سابقين يدربون ناشطين مستقبليين في أنحاء العالم، يجب على الثوريين تطوير استراتيجية مزدوجة للعمل الافتراضي والميداني. ومن دون هذه الاستراتيجية المزدوجة لا يبقى لدينا سوى فيض من المشاهير وخليط من المتسلقين من دون قادة يتمتعون بما يكفي من الثقة. والمناصب البارزة كانت على مدى التاريخ تعني ضمناً توفر حدٍّ معين من الثقة الشعبية. فباستثناء بعض الأنماط السياسية سيئة السمعة كأمراء الحرب والمديرين الآليين، لطالما ارتبط بروز القادة الكبار بحجم قواعد دعمهم. لكن هذه المعادلة ستنقلب، حيث ستأتي الشهرة بسرعة في البداية، ثم سيتوجب على الشخص أن يجمع الدعم الحقيقي والمصداقية والخبرة.

لقد سبق لنا أن رأينا هذا مع التوقعات ذاتية التحقيق لمرشحي الرئاسة الأمريكيين الذين "يستحقون ما يثار حولهم من اهتمام". فهرمان كاين غير المعروف نسبياً خارج مجال الأعمال، كان لفترة محط الأنظار عام 2012، حتى إن البعض اعتبروه منافساً جدياً، بالرغم من عدم ملاءمته للمنصب؛ الأمر الذي ثبت تلقائياً خلال أسابيع شيئاً فشيئاً، وكان من الممكن بالتأكيد كشفه مباشرةً لو دققت مؤسسة الحزب بالأمر. وستزداد أعداد مشاهير السياسة من أمثال كاين في الحركات الثورية المستقبلية، لأن الشخصيات النيزكية الكاريزماتية التي تتمتع بحضور قوي على الشبكة تطفو على السطح بسرعة كبرى. ومن دون الخبرة بصعوبات المعترك السياسي، من المرجح أن تنكشف هشاشة هؤلاء المشاهير

الثوريين بسهولة إذا لم يكن وراء بريقهم جوهر حقيقي.

ستتعاطى الحركات المعارضة مع التحدّي المتمثّل بالعثور على قادة قادرين على الاستمرار وفقاً لمكان تواجدها وحجم الموارد المتوفرة لها. ففي البلدان التي تعاني فيها الحركات الثورية من قلة التمويل وتجد نفسها في قبضة الحكومة، سيصعب التنقيب بين الجماهير عن قادة أصليين. أما الحركات المستقلة التي تمتلك ما يكفي من الموارد، فيمكنها تكليف مجموعة من المستشارين بتحديد من يتمتعون بفطرة القيادة ومساعدتهم بعد ذلك على تطوير المهارات والشبكات التي يحتاجون إليها. فعلى خلاف المستشارين السياسيين المعلبين الذين نشاهدهم اليوم، سيكون هؤلاء حملة درجات في الهندسة وعلم النفس الإدراكي، وستتوفر لديهم المهارات التقنية التي تجعلهم أكثر تمكناً بكثير في مجال استخدام البيانات لبناء الشخصية السياسية وتشذيبها. لذا، سيتناولون مرشحاً واعداً يتمتع بحضورٍ أكبر مما يتناسب مع مصداقيته، وسيقيسون إمكاناته السياسية بطرقٍ عديدة. حيث سيعملون على تعزيز خطاباته وكتاباته باستخدام برمجيات متطورة لاستخراج المعالم* وتحليل التوجهات، وسيقومون بتخطيط عمل دماغه لتحديد طريقة تعامله مع الضغط والإغواء. وسيطبقون تشخيصات متقدمة لتقييم مواضع الضعف في مخزونه السياسي.

ستشكل مجموعات ومنظمات ناشطة كثيرة جبهةً افتراضية أكثر هيبة بكثير من واقعها المادي. فتخيل تشكيل مجموعةٍ معارضة بعد أيام قليلة على حدوث ثورة في الجزائر تنجح في تجنيد مسوقين رقميين بارعين، ومصممين من المهاجرين الجزائريين في مارسيليا. وتتكون المجموعة الأساسية من خمسة أعضاءٍ فقط، جميعهم في العقد الثاني من عمرهم، ومتخرجون من الجامعة للتو، ويكاد لا يكون لديهم أي اطلاع سابق في مجال السياسة. ومع أن منظمتهم لا تمتلك سجلاً لتاريخها، إلاّ أنها مع منصتها الرقمية المتطورة تبدو للعامّة منظمة مندفعة ذات كفاءة وعلى صلات واسعة؛ في حين تكون في الواقع غير منظمة، ولا تمتلك رؤية، وغير جاهزة بشكلٍ عام لتولي أية مسؤولية حقيقية. فبالنسبة إلى مجموعات كهذه، سيتسبب الفرق بين حضورها على الشبكة وقدراتها العملياتية الفعلية بتباطؤ التحركات التي تشرع بها وتأخيرها. وفي حالاتٍ متطرفة، قد نشهد حركاتٍ كاملة تبدو على الشبكة وكأنها تمثل خطراً حقيقياً على النظام، بينما هي في الحقيقة لا تتعدى كونها توظيفاً ذكياً للتقانة لا يمثل أي تهديد أياً كان شكله. لكن المجموعات المعارضة التي لا تستطيع في نهاية المطاف النهوض بأعبائها، وترفع سقف التوقعات، وتولّد أملاً كاذباً حول فرص نجاحها، قد يكون ضررها أكبر من نفعها؛ حيث ستمثل تشويشاً مكلفاً على بقية الشعب.

لا شك في أن كل ثورة في التاريخ كانت لها نقاط ضعفٍ تنظيمية وقادة كاذبون. لكن مثل هذه الإخفاقات قد تؤدي في المستقبل إلى زيادة خيبة أمل الشعب من المجموعات المعارضة وإيصالها إلى حدها الأقصى. وحين يفقد المجتمع ككل ثقته بالحركة الناشئة وبقدرتها على تحقيق وعودها، يؤدي ذلك إلى خنق فرصة التغيير. وإذا اجتمع ذلك مع تخلخل القيادة والتباين بين الجبهتين المادية والافتراضية،

فستتآكل فرص الحركة في الحصول على الدعم والنجاح في بلدها، وسيؤدي توفر المعلومات والاتصالات لدى مزيدٍ من المواطنين إلى جعلهم نقديين ويقظين إزاء الثوار كما هم إزاء الحكومة.

سيكون لهذه العين الناقدة على قوى المعارضة المحتملة أثر على عودة أبناء المهاجر والشتات أيضاً. فعادةً، يهبط المنفيون في البلد وقد أحضروا معهم دعماً دولياً، لكن إحاطتهم بحاجات شعبهم في الوطن ورغباته تكون محدودة. وكثيراً ما انتهى هذا الانفصال عن الواقع بانطفاءٍ على المستوى الشعبـي (كالعراقي أحمد شلبـي الذي كان قائداً ذات مرة) أو بصراعات شعبية كبيرة (كتلك التي خاضها حميد كارزاي في أفغانستان). ستردم الاتصالات المتزايدة الهوة القائمة بين مجتمعات الشتات والشعب في الوطن، أي إن المنفيين العائدين الساعين إلى التأثير على العملية الثورية سيجدون أنفسهم أفضل تجهيزاً للتواصل مع اللاعبين المحليين، هذا من جهة. ومن جهةٍ أخرى، ستكون الشعوب في الوطن أكثر اطلاعاً على شؤون المنفيين العائدين (الذين سيكونون بلا شك قد أنتجوا آثاراً كبيرةً من البيانات على الشبكة تبين خلفياتهم ونشاطاتهم)، وستستخدم هذه المعلومات لتركيب سرديات تحكي عنهم قبل وصولهم.

تخيل أريتريًّا بارزاً في الشتات جمع ثروةً من صناعة الإعلام الغربية يقوم بحشد جمهور ناخبين عريض مع الكثير من الداعمين على الإنترنت، سواء أكان الدعم دولياً أو في الوطن. فقد يجد صعوبةً في إيجاد جمهور ناخبين على الأرض في أريتريا لأن الكثيرين من المواطنين المحليين قد يشكّون في خلفيته، وفي اتصالاته بوسائل الإعلام الدولية. ووعوده التي كانت فعالةً في الدائرة الدولية وبين جمهوره على الشبكة، قد يكون وقعها أجوف لدى الشعب في الوطن. فعندما يعود إلى بلاده متوقعاً أن يجد الطريق معبدةً نحو مستقبلٍ سياسي، من المحتمل جداً أن يجد آماله قد بدأت بالتلاشي مع انفضاض المواطنين المحليين عنه، وتفضيلهم منافساً له يستطيعون التواصل معه على نحو أفضل.

سينجح من بين القادة المرتبطين بالشتات أولئك الذين يتبنون نموذجاً هجيناً يتناول تطلعات الناخبين الافتراضيين المادّيين على حدٍّ سواء، ويعمل على إرضائها نوعاً ما. وسيكون كسب هاتين المجموعتين والاستفادة منهما تحدياً، لكنه سيكون حاسماً لتحقيق قيادة قابلة للاستمرار في العصر الرقمي.

ستؤدي موجة من الانطلاقات الثورية الكاذبة إلى دفع الأجيال المتعاقبة إلى مطالبة المجموعات المعارضة، ليس بالرؤية فقط، بل وبخطة تفصيلية تبيّن كيف تنوي هذه المجموعات بناء البلد الجديد. وستكون مثل هذه المطالب في محلها؛ خصوصاً مع المنظمات المعارضة الجديدة التي لا يزال ينقصها السجل التاريخي، ولا يزال عليها أن تبين حسن نيتها للشعب. وسيكون ذلك بدوره - وبشكلٍ طبيعي - بإيحاء من التوجهات التقانية السائدة؛ من شفافية إضافية، ووصول حر للمعلومات. وسيتصرف الداعمون المحتملون على نحو أشبه بالمستهلكين، فلن ينقادوا بالمثاليات السياسية بقدر ما ينقادون بالتسويق وتفاصيل المنتج. وستتاح أمام المرء طرق كثيرة توصله إلى القيادة (على الأقل اسمياً). وبوجود كل هؤلاء المرشحين

للقيادة، ومع محدودية الفرص المتاحة، سيمنح الناس ولاءهم ويسحبونه بعد إجراء حساباتٍ لا ترحم. لكن المنافسة ستكون صحيّةً بالنسبة إلى المجموعات المعارضة، كما هي بالنسبة إلى الشركات.

سيتوقع المتظاهرون المستقبليون الباحثون عن قائد من أية مجموعة معارضة جادة أن تقيم مؤسستها على الشبكة، حيث تقدم توضيحاً لهوية الوزراء المستقبليين، ولكيفية تنظيم الجهاز الأمني وتوزيع الخدمات والبضائع. إذا كان بمقدور قادة المعارضة اليوم، وخصوصاً في البلدان ذات الانتشار البطيء للاتصالات، أن يعطوا تصريحات وتعهدات غامضة مدعين أنهم يعرفون ماذا يفعلون، فإن الجمهور المطلع في المستقبل سيطالب بالتفاصيل. وحين تكون المجموعات المعارضة موجودة قبل بدء الثورة (سواء أكانت داخل البلاد أم في المنفى) فسيكون من الحكمة أن تحضّر نفسها بصدق. ولن تكون اختبارات الجاهزية للحكم مجرد تمارين، حيث سيتم تناول المخططات بحرفيتها كأساس للنظام الجديد. والمجموعة التي لا ترغب في تحقيقها، أو لا تستطيع تنفيذها بكفاءة، قد لا تلقى سوى ثناء فاتر على مهاراتها في تنظيم الجماعة. لكن مصداقيتها في القيادة والحكم ستوضع بلا شك موضع تساؤل.

حتى حين تقدم حركة معارضة مخططات تفصيلية ذات مصداقية، وتضم بين صفوفها قادةً يتمتعون بمهاراتٍ حقيقية، سيبقى هناك عدد من المتحولات التي لا يمكن التحكم بها، والتي قد تُخرج الثورة عن مسارها. فالتوترات القبلية والطائفية والإثنية تعتمل عميقاً في كثيرٍ من المجتمعات، وتبقى حقل ألغامٍ خطراً مهما كان عابره حذراً. وأيضاً ثمة مفسدون داخليون وخارجيون - كالمجموعات الإرهابية، والميليشيات، والعصاة، والقوى الخارجية - يستطيعون تخريب الأوضاع الأمنية. وبما أن الثورات التي تحصل نتيجة سوء الاقتصاد أو السياسة المالية كثيرة، فإن أقل تعديلٍ اقتصادي (سلباً أو إيجاباً) قد ينتشر صداه عبر البلاد ويدفع المحتجين إلى تغيير آرائهم.

ثم تأتي هاوية الآمال المحبطة. فحتى حين تنجح الثورة في
ويأتي لاعبون جدد إلى السلطة، ويصل التفاؤل الشعبـي إلى ذروته، قليلةٌ هي الحكومات التي ستكون قادرةً على إرضاء آمال الشعب وتطلعاته. ونتيجة انخراط ملايين كثيرة إضافية من الشعب في الثورات الشعبية - الأمر الذي يعود في جلّه إلى الاتصالات - سيزداد عدد أولئك الذين يشعرون بالإقصاء الظالم من العملية السياسية بعد انتهاء الثورة.

وهذا ما شاهدناه عن كثب في ليبيا وتونس عندما قابلنا ناشطين ووزراء في الحكومة. فكلتا المجموعتين لم تكونا راضيتيْن، ولم تشعرا بأنهما تنالان التقدير الذي تستحقانه. وبعد الثورة في مصر، كان الكثيرون منـزعجين من طريقة قيادة الحكام العسكريين الممثلين في المجلس الأعلى للقوات المسلحة للبلاد بعد مبارك، إلى درجة أنهم أعادوا احتلال ميدان التحرير الذي شهد الاحتجاجات الأصلية عدة مرات. وعندما وجد الشعب أن خياراته محدودة في الانتخابات الرئاسية الأولى في مصر بعد الثورة (ما بين أحمد شفيق رمز الجيش، ومحمد مرسي رمز الإخوان

المسلمين)، تعمّق لديه اليأس والشعور بالإقصاء. ونتيجة المدى الذي يستطيع الناس الوصول إليه في شعورهم بالمشاركة اليوم عبر الاتصالات، سيرتفع سقف توقعاتهم إلى درجة غير مسبوقة.

ستحاول الحكومات الجديدة الاستجابة لمطالب المحاسبة والشفافية هذه عبر اتخاذ مبادرات التي قد تشتمل على نشر جداول المواعيد اليومية للوزراء، والتفاعل مع المواطنين عبر المنتديات الشبكية، وإبقاء خطوط الاتصالات مفتوحةً قدر الإمكان. إلا أن بعض المواطنين لن يرضيهم أي شيء، وبين هؤلاء ستجد الطغمة السياسية المُزاحة شبكة دعمها على الإنترنت. وسيستغل الموالون الأذكياء هذه الفجوة في الآمال من خلال البقاء على تواصلٍ مع الشعب عبر الشبكة، وتغذية شعوره بالضَّيم سعياً إلى استعادة النظام، وقد يصلون في النهاية إلى تشكيل حركة المعارضة الجديدة على الشبكة.

القمع والاحتواء في العالم الافتراضي

ستبحث الدول، وقد حاصرتها التهديدات الثورية من كل حدب وصوب، عن حلول سريعة لمعالجة التمردات التي تطفو على السطح. وسيتوجب عليها أن تتعلم الإبداع، فالطرائق التقليدية - كالقمع والتحجيم والتعتيم - ستفقد فعاليتها باضطراد مع انتشار الاتصالات. وستفقد الاستراتيجية الاستبدادية البالية، القائمة على قمع العصيان بالعنف وبمحاصرة قادته، الكثير من واقعيتها في عصر الاحتجاجات الرقمية والنشاط عبر الإنترنت والبث الحي للشهادات. والتاريخ يبيّن أن حملات القمع، مع بعض الاستثناءات الشهيرة (ساحة تيانانمين عام 1989، ومجزرة حماه عام 1982) نادراً ما تسجل كفيديو، وأن نشر الصور وأفلام الفيديو خارج البلاد في غاية الصعوبة. فعندما كان النظام يسيطر على قنوات الاتصال ووسائل الإعلام والحدود، كان التسريب إلى الخارج ضرباً من المستحيل.

ما إن أصبحت الأجهزة النقالة والإنترنت سمة من سمات الثورات والاحتجاجات الشعبية، حتى عدلت الأنظمة استراتيجيتها، فقامت بإغلاق الشبكات؛ وهذا تكتيك بدا ناجعاً لدى الكثير من الحكومات في البداية، وفي مقدمتها النظام الإيراني خلال الاحتجاجات التي تلت انتخابات عام 2009 حين نجح الإغلاق شبه التام للشبكة في احتواء حركة المعارضة المتنامية احتواءً فعالاً. وبعد ذلك بأقل من عامين كان لدى الرئيس المصري حسني مبارك ما يكفي من الأسباب للاعتقاد بأن حملة القمع الافتراضية ستضع حداً للحراك الثوري في ميدان التحرير، لكن هذه الاستراتيجية - كما تبين القصة التالية - أعطت نتائج عكسية منذ البداية. ففي الساعات الأولى من الثامن والعشرين من كانون الثاني عام 2011، قام النظام المصري الذي كان يتوقع احتجاجات معارضة واسعة النطاق في ذلك اليوم، بإغلاق جميع اتصالات الإنترنت والاتصالات النقالة في البلاد. وعنونت إحدى المدونات التي تناولت الحدث في بدايته *. وكان النظام قبل ذلك ببضعة أيام قد حجب مواقع الشبكات الاجتماعية وخدمة بلاكبيري على الإنترنت، وأتت هذه الخطوة لتجعل

العزلة تامة–** . وتأثرت بذلك جميع مزودات خدمة الإنترنت الأربعة في البلاد (لينك إيجيبت، والاتصالات المصرية، واتصالات مصر، وفودافون ريا)، كما تم إيقاف خدمة الهاتف النقال من قبل مشغلي الاتصالات، وأصدرت فودافون المصرية، أكبر شركات الاتصالات في البلاد، تصريحاً في ذلك الصباح يفيد: "إن جميع مشغلي الاتصالات النقالة في مصر قد أبلغوا بإيقاف خدماتهم في مناطق معينة. ووفقاً للتشريعات المصرية، يحق للسلطات إصدار مثل هذا الأمر، وليس أمامنا سوى الامتثال له".

بما أن الحكومة المصرية كانت تسيطر مسبقاً على الاتصالات المادية القليلة التي تربط البلاد بالعالم الخارجي (ككابلات الألياف الضوئية الموجودة في بناء واحد في القاهرة)، كانت عملية الإغلاق عمليةً بسيطةً لا تتطلب سوى إغلاق هذه المنافذ وإبلاغ المشغلين والمتعهدين الكبار بالمطلوب. وقد كُشف النقاب بعد ذلك عن أن النظام قد وضّح للشركات، مثل فودافون، من دون لبس أن عدم إذعانها لأمر الإغلاق سيدفع الحكومة المصرية، عبر شركة الاتصالات المصرية المملوكة للدولة، إلى قطع خدمتها مادياً عبر البنية التحتية للاتصالات في البلاد (الأمر الذي قد يدمر قدرة فودافون على التشغيل، ويتطلب قدراً كبيراً من الوقت للعودة عنه). لقد أُخذت مزودات خدمة الإنترنت وشركات الاتصالات على حين غرة. فلطالما كانت الحكومة مؤيدةً لانتشار الإنترنت وخدمات الاتصالات النقالة عبر مصر، لذا إن أياً من هذه الشركات لم يكن قد أعدّ خطة للطوارئ. لقد كانت حركة غير مسبوقة في التاريخ، إذ كانت دول أخرى تتدخل بخدمات الإنترنت المقدمة لشعوبها، لكن أياً منها لم تُجر مثل هذا الفصل التام والمنسق من قبل.

ثم جاء دور الحركة في الرد. فكما نوَّه عدد من المصريين والمراقبين الخارجيين في ما بعد، كان إغلاق الشبكة هو الذي هيّج حركة الاحتجاج عملياً، لأنه دفع الكثير من الناس الغاضبين إلى الشوارع. وهو ما يتفق معه فيتورو كولاو، رئيس مجلس إدارة فودافون حين قال لنا: "إن الاصطدام مع الشعب كله حول شيءٍ يعتبره الجميع أساسياً، وتم أخذه منهم كلياً، ولدّ رد فعلٍ غاضباً وسلبياً على نحوٍ لم تتوقعه الحكومة". وهو ما أكده العديد من الناشطين المصريين الذين قالوا بالفعل إن "مبارك" لم يكن يروق لهم لكنها أيضاً لم تكن معركتهم، لكن بعد ذلك "حرمني مبارك من الإنترنت، فجعلها معركتي، وذهبت إلى ميدان التحرير". فمنح هذا الفعل المثير زخماً للحركة لا يستهان به. ولولا ذلك لربما اتخذت الأحداث في مصر مساراً مختلفاً تماماً.

قال كولاو إنه عندما وصل طلب النظام بإغلاق الشبكة كانت أول خطوة قامت بها فودافون هي "التأكد من وجهة النظر القانونية؛ للتأكد من أن ما أمامنا طلبٌ شرعي. فمن الممكن الطعن فيه، لكن يجب أن يكون قانونياً على الأقل". فجميع مزودي الاتصالات يحتاجون إلى عقود ترخيص مع الدولة، لذا عندما أدركت فودافون أن الطلب شرعي، لم يبقَ لديها خيار. "ربما لم يعجبنا الطلب، لكن عدم الالتزام به كان سيعد خرقاً للقانون".

بعد ذلك بوقت قصير، وبينما كانت خدمة الإنترنت والهواتف النقالة متوقفة في

مصر، وجدت فودافون نفسها أمام اختبار جديد، حيث بدأت الحكومة تمهد لإرسال الرسائل عبر منصة خدمة الرسائل القصيرة الخاصة بالشركة وبمشغلين آخرين. وكانت تلك هي اللحظة التي بدأت فيها فودافون تلعب دوراً إيجابياً كما أخبرنا كولاو، حيث كانت نبرة الحكومة في البداية إجرائيةً كما قال لنا، مثل"يوجد منع تجول الليلة بين السادسة والتاسعة". "من الممكن تنفيذ مثل هذا الأمر"، يوضح كولاو. وجاء النوع الثاني من الرسائل بشحنة وطنية، حيث ورد فيها شيء مثل "لنتحابّ ونحب أمتنا"، لا بأس بذلك أيضاً يقول كولاو، "لكن الرسائل أصبحت في ما بعد سياسيةً ومنحازة على نحو لا يصدق. وعندها، لم يعد بالإمكان أن نطلب من كوادر فودافون المحلية أن تخبر حكومتها بأننا لا نستطيع الامتثال للقانون المصري، رفعنا الأمر إلى الخارجية المصرية، وهيلاري كلينتون، وحكومة المملكة المتحدة، وبعد ذلك إلى مجموعة فودافون بـي.أل.سي (الشركة الشريكة) التي أصدرت بياناً قالت فيه إننا نرفض طلب الحكومة. وكان ذلك ما أوقف الرسائل القصيرة. ثم أوقفت الاتصالات الصوتية لدينا لمدة 24 ساعة، وأوقفت خدمة الرسائل القصيرة لأربعة أيام أو خمسة، فقد كانت الرسائل القصيرة هي التي تمثل تهديداً بالنسبة إليهم".

سيستقي المشغلون والحكومات على حدٍّ سواء درساً من فشل تكتيك الإغلاق في مصر. فقد أدى إلى تعبئة الجماهير داخل البلاد، وإلى إثارة سخط المجتمع الدولي في الخارج، ولم تمر أيامٌ معدودة على الإغلاق حتى كانت الشركات، بالتعاون مع الناشطين، قد طورت طرقاً بديلة تسمح للمواطنين المصريين بالاتصال مجدداً، وإن بشكلٍ مرقع. فقامت منظمة غير ربحية مقرها في باريس تدعى شبكة البيانات الفرنسية بفتح الإنترنت عبر اتصالات الطلب الهاتفي (تتاح لأي شخص يتصل من خط أرضي دولي)، بينما أطلقت غوغل خدمة التغريد عبر الهاتف باسم سبيك تو تويت التي كانت تسمح للمتصلين باختيار رقم من ثلاثة أرقام وترك رسالة صوتية يتم نشرها بعد ذلك على شكل تغريدة في تويتر.

أخبرنا فيتوريو كولاو بعد الأحداث في مصر أن المشغِلين الرئيسين للاتصالات اجتمعوا لمناقشة كيفية الحؤول دون تكرار هذا الأمر مرة أخرى، وكيف يمكنهم اتخاذ موقفٍ مشترك في حال حدوث ذلك. وأخيراً، كما يقول "قررنا أنّه لا بد من مناقشة ذلك ضمن الاتحاد الدولي للاتصالات [الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية][الوكالة الأممية المتخصصة بالاتصالات العالمية] لتحديد قواعد الانخراط بدقة"، ولا بد أن حكومات أخرى في المستقبل ستتذكر حادثة الإغلاق المصرية، وستعيد النظر في تقييمها فرص النجاة التي ستتاح لها لو منعت الاتصالات عن شعوبها. علاوةً على ذلك، ومع ازدياد شعبية المنصات الثنائية وغيرها من منصات الاتصالات التي تعمل من دون الشبكة التقليدية، سينحسر أثر إغلاق شبكات الاتصالات انحساراً هائلاً. وقد تفكر الحكومات غير العقلانية أو الأنظمة المصابة بالذعر مع ذلك

باتخاذ خطواتٍ متطرّفة كقطع الاتصالات على الحدود حرفياً، أي قطع كابلات الألياف الضوئية أو تدمير الأبراج الخلوية. لكن خطوةً كهذه ستلحق ضرراً خطيراً باقتصاد البلاد (حيث ستتوقف جميع الأسواق المالية وأسواق العملات والأعمال التجارية التي تعتمد على البيانات الخارجية في عملها)، ممّا سيجعل أي نظام يحجم عن اتخاذها على الأرجح.

لكن صفة الحكومات الاستبدادية هي الدهاء قبل أي شيء آخر. لذا، ستجد طريقة لتحقيق النفوذ واستغلال الثغرات لمواجهة الشعب المتململ والتحديات الثورية التي يفرضها بالتأكيد. وستعمل الدول على تطوير طرائق جديدة أكثر تحايلاً وغدراً. وسيطبق كثير منها استراتيجية "إذا لم تنل منهم، فانضم إليهم" بأن يتسلل عبر الإنترنت بدلاً من أن يحدّ من الوصول إليها. وكما ناقشنا سابقاً، إن بإمكان الدول تحقيق تفوق لا يستهان به على مواطنيها في عصر ثورة البيانات نتيجة الكم الذي يمكنها الوصول إليه من معلوماتهم. وعندما تخشى حكومة ما من نشوب تمرد، يمكنها تفعيل عمليات مراقبة الإنترنت لديها والتصيد في شبكات الوسائط الاجتماعية بحثاً عن ناشطين مفوّهين أو معارضين بارزين لتغري بعضهم وتعتقل غيرهم، أو اختراق مواقع التعبئة الهامة وتغذيتها بمعلومات مضللة، أو السيطرة على كاميرات وب على الحاسب المحمول أو اللوحي لشخص معارض للتنصت على تصرفاته ومشاهدتها من دون علمه، أو التدقيق في المدخلات المالية على منصة رقمية لتحديد مصادر الدعم الخارجي. وقد يعتبر الاختراق المبكر الفاصلَ بين مظاهرة صغيرة وتمرد على المستوى الوطني.

حتى إذا تغيرت طبيعة القمع الافتراضي، فإن عمليات القمع الفيزيائية ستبقى ثابتة من ثوابت الكتاب الأمني لدى الدولة القمعية. وليس بإمكان التقانة أن تقف في وجه الوحشية الميدانية كما تبين لنا الأمثلة المريعة القادمة من سوريا خلال حملة القمع التي امتدت لسنوات. ومهما بدا ذلك مستحيلاً، فإن المجتمع الدولي قد يفقد إحساسه تجاه العنف الذي يتضمنه المحتوى الصوري المنشور، حتى إذا كان تدفق الصور وأفلام الفيديو المرعبة يزداد في الواقع مع مرور الوقت. بشكل عام، إنّ الحكومات التي لا تزال تحاول حماية مصداقيتها وإنكار مثل هذه الجرائم ستجد في عمليات القمع الوحشية مجازفة أكبر في العصر الرقمي. فزيادة الشفافية عبر المنصات الشبكية العالمية تحمي المواطنين بالفعل، وهو ما سيصبح - على ما نأمل - الحالة السائدة مع تحسن أدوات مثل برمجيات التعرف على الوجوه. فقد يتشجع ضابط في الجيش على إبداء بعض الالتزام، أو حتى الانشقاق، إذا علم أن صورةً واحدة يتم التقاطها في التوقيت الصحيح بجهاز أحد المواطنين كافية لتحديد هويته وإحراجه دولياً. ينطبق الأمر نفسه على الميليشيات المدنية غير الرسمية التي تتورط في العنف لصالح النظام، كالعصابات الزيمبابوية التي تقاتل لصالح حزب روبرت موغابـي زانوبف.

بدلاً من استراتيجية التسلل (أو على الأقل إلى جانبها) نتوقع أن تتبع دول كثيرة استراتيجيةً سنسميها الاحتواء الافتراضي. فلتخفيف الضغط الذي يمارسه شعب ثائر ومطلع ستتوصل الدول إلى أنه بدلاً من حجب الخدمات برمتها قد يكون من

الأفضل ترك نافذة مفتوحة تسمح للمواطنين بالتنفيس عن مظالمهم على الإنترنت، لكن - وهذا هو الأهم - إلى درجة معينة فقط. حيث ستسمح الأنظمة في المستقبل ببعض المعارضة على الشبكة، سواء أفعلت ذلك عبر إصلاح قوانينها، أو بعدم المعاقبة على الكلام، لكن ضمن شروطها الخاصة وعبر قنوات محددة تسيطر عليها. ففي نهاية المطاف، ليس من الوارد أن يشكل منح ناشطٍ بيئي في بوليفيا مساحةً يشتكي عبرها من مخاطر التصحر تهديداً كبيراً لقوة الحكومة.

للوهلة الأولى، يبدو أن الجميع سيبقى رابحاً مع فضاءات الافتراضية التي يتم إنتاجها؛ إذ سيشعر المواطنون بالمشاركة على نحوٍ أعمق، وربما بدرجةٍ جديدة من الحرية، بينما ستربح الحكومة نقاطاً تساعدها على الإصلاح (عبر تجنب ثورةٍ كاملة أو كبحها على الأقل)، وربما تدرك بعض الدولِ القمعية بالفعل قيمة الإصلاح وتقدم تغييرات سياسية من دون مواربة. لكن دولاً كثيرة أخرى لن تفعل ذلك، ليس فقط لأن المؤشرات التي يمكن استقاؤها لن تكون صادقة (حيث لن تكون مثل هذه الحكومات مكترثة بالتغذية الراجعة من المواطن)، بل أيضاً لأن الدولة لن ترى في مثل هذه المساحات سوى فرصة لجمع المعلومات الاستخباراتية. فالأنظمة تدرك بالفعل القيمة الاستراتيجية للسماح بالنشاط على الشبكة بما يسمح بتنظيم الاعتقالات. فقبل عقدٍ من الزمن، كانت شرطة الآداب المصرية ترمي طعوماً في غرف الدردشة ومنتديات الإنترنت، وتستخدم هويات مزيفة للإيقاع بالمواطنين المثليين واستدراجهم إلى محل ماكدونالد في القاهرة لمباغتتهم وإلقاء القبض عليهم. وفي عام 2011 بعد الثورة التونسية، استجاب عدد من المعارضين الصينيين لدعوةٍ على الشبكة إلى نسخةٍ صينية من الاحتجاجات تقام أمام سلاسلٍ أمريكية شعبية مثل مقاهي ستار باكس. وانتشرت دعوات التعبئة عبر الوسائط الاجتماعية والمدونات الصغرية الصينية حتى وصل خبرها إلى الشرطة، وعندما وصل الناشطون إلى المكان المتفق عليه واجههم عدد غفير من رجال الشرطة الذين اعتقلوا كثيرين منهم. ولو أن الحكومة قضت على هذا النشاط الشبكي مباشرةً بعد ملاحظته لما تمكنت الشرطة من تقفي أثر النشاط الافتراضي وإيجاد المعارضين الماديين.

في إطار استراتيجيات الاحتواء الافتراضي ستبدر من الدول سلسلة من أمارات الشفافية، حيث ستتخلى عن الفتات، بينما ستبقي في قبضتها معظم المعلومات التي تمتلكها. وسيُحتفى بهذه الدول لما تقوم به من فتح مؤسساتها، وحتى الكشف عن جرائمها السابقة. وقد ترغب حكومة معروفة بفسادها الداخلي بالظهور بمظهر من يفتح صفحةً جديدة بالكشف علناً عن رشوةٍ قَبِلها أحد قضاتها أو أحد زعمائها السابقين. وقد يقوم نظام قائم على دولة الحزب الواحد بإصدار بعض المعلومات الدقيقة، لكن غير المُدينة أو غير المفيدة حقاً، مثل تفاصيل ميزانية وزارة الصحة لديه. وسيظهر رجال يكونون بمثابة كبش فداء؛ يتحملون المسؤولية، ويمتصون الغضب الشعبـي بينما ينجو النظام. ولن تصعب على هذه الأنظمة فبركة وثائق تبدو شفافةً وسجلات، ففي غياب معلوماتٍ تناقضها (كالوثائق الأصلية المسربة) لن يكون هناك أمل كبير في إثبات زيفها.

سيكون التحدي الحقيقي أمام الدول التي تعتمد طريقة الاحتواء الافتراضي هو التمييز بين منافذ الترويح الشعبية وبين المعارضة الحقيقية على الشبكة. يستخدم مهندسو الحاسب مصطلح لوصف الإشارات التي قد تكون قوية جداً لكنها لا تحمل أية بيانات مفيدة. وستواجه الحكومات الاستبدادية نسخة سياسية من هذا الضجيج عندما تسمح بمزيد من الحرية في المناقشات على الشبكة. ففي المجتمعات المنفتحة، ثمة قوانين متعلقة بحرية التعبير وبلغة الكراهية تعرّف إلى حدٍّ كبير الحدود المقامة على المواطنين. أما في البلدان المغلقة، فإن النقص في السوابق القانونية للخطاب المسموح به يجعل الحكومة تعمل على نحو أعمى نوعاً ما، حيث سيصعب على الدول تحديد ما يخبئه الناس وراء كلماتهم من نوايا على الشبكة. فحين لا يكون هؤلاء معارضين، ولا تربطهم صلات بمجموعاتٍ معارضة، ولا يتميزون عن غيرهم بأية طريقة، فكيف يمكن للحكومة الملتزمة حديثاً بالحوار أن تستجيب من دون مبالغة؟ إن هذا الغموض الذي يكتنف الضجيج الرقمي سيكون بطاقة رابحة كبيرة بيد السلطات التي تكافح لتقييم الحالة أولاً للمبادرة إلى الفعل. وقد يكون الفهم الخاطئ الذي يتجلّى بالمبالغة برد الفعل أو بالتقصير فيه، قاتلاً بالنسبة إلى النظام. وتجاهل تصعيد ما على الشبكة قد يحوله إلى عاصفةٍ في العالم الحقيقي. والقسوة في ردع شخصٍ يمزح على الإنترنت قد تؤدي إلى نشوء حركة على الشبكة وإعطائها قضية تجتمع عليها بعد أن كانت بلا أي زخم على أرض الواقع.

لا ربيع بعد اليوم

مع دخول المزيد من المجتمعات إلى الشبكة، سيبحث الناس عن أعراض تنم عن أوبئة ثورية إقليمية. ويراهن البعض على أن أمريكا اللاتينية ستكون المنطقة التالية؛ لما تعاني منه من حدة في التباينات الاقتصادية، وضعف الحكومات وهرم القيادات، إضافة إلى حجم الشعوب التي تتحدث اللغة نفسها. بينما يطرح آخرون أفريقيا ذات الدول الأكثر هشاشة في العالم، والتي تشهد ارتفاعاً هائلاً في معدل انتشار الهاتف الخلوي يجعلها السوق الأسرع نمواً للهاتف النقال على الإطلاق. أو قد تكون آسيا التي تحتوي أكبر عدد من البشر الذين يعيشون في ظل نظام مستبد، وتتمتع بنمو اقتصادي سريع، وبالكثير من التوترات الاجتماعية والاقتصادية والسياسية المزمنة. وقد ظهرت بالفعل بعض بوادر تنظيم الاحتجاجات والمظاهرات في فيتنام وتايلاندا وماليزيا وسنغافورة، ولا شك في أن هذا سيستمر مع الوقت.

لكن، حتى إذا أصبحت هذه المناطق أكثر اتصالاً، واطلعت شعوبها على أحداث القوميات الأخرى ومظالمها المشتركة، فإننا لا نملك الدليل بعد على حدوث موجة جديدة من العدوى كتلك التي شهدها العالم خلال الربيع العربـي (وما من معنى مع ذلك لسهولة انتشار عدوى الاحتجاجات والمظاهرات، كما تَبين في أيلول عام 2012 عبر ردود الفعل التي أثارها الفيلم المسيء "براءة المسلمين" في عشرات البلدان حول العالم). فالعالم العربـي يتمتع بهوية إقليمية فريدة لا تشاركه فيها

مناطق أخرى، وقد عززتها المحاولات التاريخية لإقامة الوحدة، ومشاعر العروبة على مدى عقود. كما أن اللغة المشتركة والثقافة المشتركة والتشابه في الأنظمة السياسية كان لها دورها أيضاً. وكما سبق وقلنا، إن تقانات الاتصالات الحديثة لم تخترع الشبكات التي استفاد منها الناشطون والمحتجون في الشرق الأوسط، بل عززتها فقط.

إضافةً لما سبق، كانت هناك شبكات دينية راسخة أصبحت - في ظل غياب مجتمع مدني قوي في ظل الحكم المستبد - منذ البداية الكيان غير الحكومي الأكثر تنظيماً، وربما الأكثر نفعاً بالنسبة إلى المواطنين. فجميع القادة العرب الذين فقدوا السلطة في موجة الثورات قاموا ببناء نظم سياسية تخنق تطور المؤسسات، كما قاموا بتشغيلها، فصارت دور العبادة والمنظّمات الدينية هي غالباً التي تملأ الفراغ (وقد اكتسبت بذلك عداوة أولئك الحكام. وقد كانت أبرز هذه المجموعات، مثل الإخوان المصريين في مصر وحزب النهضة الإسلامي في تونس، إما محظورةً صراحةً أو خاضعةً للاضطهاد بلا رحمة من قبل الدولة لأنها تمثل تهديداً لها). وفي غمرة الثورات الأخيرة، تحولت المساجد إلى نقاط لقاء، وأضفى الأئمة ورجال الدين الشرعية على قضية المحتجين في بعض الحالات، وكان التضامن الديني بالنسبة إلى الكثيرين حافزاً هاماً على التعبئة. لكن المناطق الأخرى تفتقر إلى مثل هذه المكونات، فأفريقيا وأمريكا اللاتينية وآسيا متنوعة ومتباينة ثقافياً ولغوياً واقتصادياً أكثر بكثير من أن تحاكي النموذج العربـي. كما أنه لا توجد فيها هويةٌ إقليمية كتلك الموجودة في الشرق الأوسط. فالشبكات الاجتماعية والتجارية والسياسية أكثر محلية هناك.

إلا أنه من المستحيل ألا تلوح التغييرات في أفق جميع هذه المناطق. وقد تكون هذه التغيرات مرتبطة ببلد معين، أو قد تشتمل على طيف أوسع من النتائج لا ينحصر بتغيير النظام فقط، لكنها ستبقى عميقةً على المستوى السياسي والنفسي. فكل بلد في العالم سيشهد المزيد من المحرضات الثورية، لكن معظم البلدان ستنجو من العاصفة، لأنها حظيت بفرصة مشاهدة أخطاء البلدان الأخرى والتعلم منها. وستظهر مجموعة من الممارسات التي تفضلها الدول لتحريف الاتهامات التي ستلقيها عليها الجماهير حديثة التواصل، ولتشتيتها والرد عليها (وهذا افتراضٌ منطقي بما أن وزراء الداخلية المسؤولين عن الشرطة والأمن الوطني في الدول المستبدة يتبادلون الزيارات لتشارك المعارف والتقنيات)، فمواضيع عدم المساواة في الدخل، والبطالة، وارتفاع أسعار الغذاء، ووحشية الشرطة موجودةٌ في كل مكان. وسيكون على الحكومات اتخاذ تعديلات وقائية على سياساتها ورسائلها لتعالج المطالب الشعبية، ولتستجيب لها بسرعةٍ أكبر مما اعتادت عليه. وحتى في المجتمعات المستقرة نسبياً، يستشعر القادة الضغط الذي يفرضه تواصل المواطنين، وهم يدركون الحاجة إلى الإصلاح أو التأقلم مع العصر الرقمي الجديد لأنه ما من حكومةٍ منيعةٍ على هذه التهديدات القادمة.

وما من أحد يستوعب هذا الارتباط بين الضغوط السياسية والتحديات التقانية أفضل من رئيس الوزراء السنغافوري لي حسين لونغ، القائد الإقليمي،

والمعلوماتي المتدرب في آنٍ معاً، الذي قال لنا "تفيد الإنترنت في تنفيس الضغط لكنها قد تستخدم أيضاً لإضرام نيرانٍ جديدة. والخطر الذي نواجهه في المستقبل هو أن معارضة أي شيء ستكون أسهل بكثير من دعمه. فالشباب في كل مكان"، يوضح لنا، "يرغبون دائماً بالمشاركة في شيءٍ لطيف، وإمكانية معارضة السلطة بطريقة اجتماعية تعني أن الشباب ما عادوا بحاجة إلى خطة، فقد أصبح في غاية السهولة أن تتصعد أحداث صغيرة لتتحول إلى نشاطات كبيرة على الشبكة يمكن استغلالها من قبل المجموعات المعارضة".

أشار إلى حدث طرأ مؤخراً في بلاده دُرِج على تسميته "بوابة الكاري". يقول : "اختلف مهاجرٌ صيني مع سنغافوري من أصل هندي على الطبخ بالكاري لأن رائحته تتسرب عبر الجدران"، حيث اعتبر الرجل الصيني طبخ جاره باستمرار باستخدام الكاري تصرفاً مستهتراً لا يراعي فيه الآخرين ولجأ الطرفان، "على الطريقة السنغافورية المعتادة"، إلى وسيط يحل خلافهما. وتم التوصل إلى اتفاق ينصّ على أن لا يطبخ الهندي بالكاري سوى عندما يكون جاره خارج المدينة. كانت تلك نهاية القصة، إلى أن قام الوسيط بعد سنوات بسرد القصة على الملأ، مما أغضب الجالية الهندية في سنغافورة، التي أثار سخطها أن يُملي رجلٌ صيني على الناس متى يطبخون باستعمال الكاري ومتى لا يستعملونه. وتصعّد الموقف بسرعة، فوفقاً للسيد : "ما بدأ على شكل صفحة إعلانٍ لليوم الوطني لطبخ الكاري حصد الآلاف من الإعجابات والمداخلات، وأثار حركةً فيروسية خطفت أنظار البلاد برمتها". ومن حسن حظ ، فإن الحراك الذي جرى على الشبكة بسبب الكاري لم يقد إلى احتجاجات في الشوارع، مع أن الخطابات كانت مشحونةً للغاية في ذلك الوقت.

لم تكن للاحتجاجات في سنغافورة صلة كبيرة بالكاري أو بأي شيء يتصل بالمخاوف المتنامية من قدوم الأجانب (وخصوصاً من البلد الأم الصين) إلى البلاد واستيلائهم على فرص العمل. ومن غير المفاجئ أن المجموعات المعارضة التواقة للدفع بهذه الأجندة قد وجدت في بوابة الكاري فرصة يسهل اغتنامها. ففي بلد مثل سينغافورة يفاخر باستقراره وفعاليته وحكم القانون فيه، كشف انتشار هذا الغضب بين الكثير من مواطنيه عن نقطة ضعف في النظام. فحتى في فضاء خاضع لسيطرة محكمة مثل سينغافورة، ليس للتشريعات الحكومية والأعراف الاجتماعية أثر كبير في العالم الافتراضي. أما فقد وجد في الأحداث نذيراً لموجة عارمة من التعبير على الإنترنت تدرك القيادة السينغافورية أن لا رادّ لها. فإذا كانت الحكومة السينغافورية تستشعر غليان المجتمع المدني حديث الاتصال، فلك أن تتخيل مدى التوتر الذي تعيشه الحكومات الأكثر هشاشة في أنحاء أخرى من العالم.

سألنا عما سيكون عليه برأيه رد فعل الصين على هذا التحول، علماً أنه خلال عقد من الزمن سيصبح نحو مليار مواطن صيني متصلين بالإنترنت ضمن مجتمعٍ خاضعٍ لرقابةٍ عالية. فرد بالقول: "إن ما يحدث في الصين ليس لأحد سيطرة كاملةً عليه؛ حتى الحكومة الصينية نفسها. ستمر الصين بأوقاتٍ عصيبة تضطر فيها إلى مجاملة جميع هذه الأصوات الجديدة، وسيكون تحول المتصلين بالإنترنت بين

صفوف الشعب، من أقلية إلى أكثرية، صعباً على القادة". وبمناسبة الحديث عن القيادة أضاف: "فالأجيال القادمة من القادة الصينيين لن تتمتع بالكاريزما وبمهارات التواصل اللازمة لتوليد الزخم لدى الشعب. وبهذا المعنى، إن العالم الافتراضي سيصبح أكثر إثارة وأهمية بالنسبة إلى الشعب الصيني مقارنةً بالعالم المادي. فالتغيير لن يأتي فقط من أشخاصٍ خارج النظام، فثمة أشخاص داخل النظام، ومن كوادر المؤسسة الصينية سيتأثرون بلَغْو الشارع، وهم أيضاً من ستكون لديهم وجهات نظرٍ متشككة في شرعية الحكومة.

إننا نتفق مع وغيره من الخبراء الإقليميين على أن مستقبل الصين لن يكون بالضرورة مشرقاً. ويرى البعض في بروز عوامل معينة مثل انحسار النمو الاقتصادي، وشيخوخة الشعب، والتغيير الذي تدفعه التقانة مؤشرات على أن الدولة الصينية ستخوض قريباً معركة بقاء ضمن شكلها الحالي. بينما يرى آخرون أن هذه التحديات الوشيكة ستحفز في نهاية المطاف المزيد من الابتكار والقدرة على حل المشكلات في الصين. إلا أنه يصعب علينا في النهاية تخيل كيف يمكن لنظام مغلق ذي 1.3 مليار نسمة مع تحدياتٍ اجتماعية - اقتصادية هائلة وقضايا إثنية داخلية ورقابة غليظة أن ينجح في النجاة من هذا التحول، والدخول في العصر الرقمي الجديد في شكله القائم حالياً. فتزايد الاتصالات سيترافق مع ارتفاع في التوقعات والمطالب، وفي القدرة على المحاسبة؛ ستعجز عن السيطرة عليها بشكلٍ كامل أكبر الدول الرقابية في العالم. وفي الحالات التي تتجاوز فيها السلطة التنفيذية حدودها، أو يتبع فيها أصدقاء النظام سلوكيات متهورة تتسبب بأذى جسدي للمواطنين الصينيين، سنشهد المزيد من التحركات الشعبية التي تطالب بالمحاسبة. ومع تحاشي الوزراء للإحراج، سيولد الضغط الذي تمارسه مدونات الويبو، وغيرها من المنتديات على الإنترنت، إلى زيادة الضغط والتغيير، مما سيكبح جماح حكم الحزب الواحد.

في حين أن الإنترنت لن تُحدث تحولاً ديموقراطياً في الصين بين ليلة وضحاها، سيؤدي ازدياد المحاسبة الشعبية إلى ممارسة بعض الضغط على النظام على الأقل، وإلى دفعه إلى معالجة المطالب الشعبية بالعدالة. وإذا شهد النمو الاقتصادي تباطؤاً ملحوظاً، فإنه سينتج فرصةً ثورية بالنسبة إلى بعض فئات الشعب. وستشهد الصين شكلاً ما من أشكال الثورة خلال العقود القادمة، لكن مدى انتشارها وفعاليتها سيعتمد على استعداد الشعب للمجازفة، سواء أفعل ذلك على الإنترنت أم في الشوارع.

قد تفلح ثورات المستقبل - أينما حدثت وأياً كان شكلها - في تغيير الأنظمة، لكنها لن تفرز بالضرورة بدائل ديموقراطية. فكما أخبرنا هنري كسنجر: "قصة الثورات هي قصة تراكم للاستياء يصل إلى حدّ انفجاري فيكنس البنى الموجودة. بعد ذلك، إما أن تعم الفوضى، أو تستعاد سلطة تتناسب عكسياً مع التدمير الحاصل على السلطة السابقة". بعبارة أخرى، بعد ثورةٍ ناجحة، "كلما دمرت السلطة، ازدادت مطلقية الثورة التي تليها"، يقول كسنجر. فبعد أن شهد ثورات ناجحة وفاشلة على مدى أكثر من أربعين عاماً، أصبحت لديه معرفةٌ عميقة بأشكالها

وخصالها. وهو يرى أن الولايات المتحدة وأوروبا الغربية هما الحالتان الوحيدتان اللتان أدى فيهما تدمير البنى الموجودة إلى إنتاج ديموقراطيات أصيلة، إذ يتابع موضحاً: "نجحت الثورات في أوروبا الشرقية لأن تجربتها مع الديكتاتورية كانت في غاية السوء، ولأن لديها سجلاً للانتماء للغرب، وهي تشكل جزءاً من التقليد الديموقراطي، حتى لو لم يسبق لها أن عاشت الديموقراطية من قبل قطّ".

مع أن كسنجر محق في مسألة تميز أوروبا الشرقية، إلاّ أنّه لا يمكننا أن نتجاهل الدور الذي تلعبه الدوافع في نجاح الثورات. فمن الإهمال استبعاد الحافز الهام للغاية المتمثل في القدرة على الانضمام إلى الاتحاد الأوروبـي. فلو لم تكن عضوية الاتحاد الأوروبـي موجودة كحافز سياسي للنخب الليبرالية وللشعوب عامةً، وأيضاً كعامل استقرار لكنا قد شهدنا على الأرجح قدراً أكبر من الردة ومن الثورات المعاكسة في عدد من البلدان المختلفة. وهو ما دفع القوى الغربية إلى توسيع الناتو وتقديم عضوية الاتحاد الأوروبـي.

إن غياب الثقافة الديموقراطية على هذا النحو يشكل أحد الأسباب التي جعلت إسقاط الأنظمة خلال الربيع العربـي يتمخض عن مجرد نسخٍ مخففة من النظم الاستبدادية كما يرى البعض، وليس عن ديموقراطيات جفرسونية صرفة. يقول كسنجر: "بدلاً من تجميع جميع السلطات في يد الدكتاتور، يقومون بتقسيم أنفسهم إلى أحزاب مختلفة، علمانية وغير علمانية، لكنهم في النهاية يجدون أنفسهم وقد هيمن عليهم حزب إسلامي واحد يدير حكومة ائتلافٍ شكلية. والنتيجة ستكون حكومات ائتلاف" - يقول مازحاً - "ترحب بها نيويورك تايمز على أنها تعبير عن ديموقراطية عظيمة". ثم يضيف بجدية: "وفي نهاية هذه العملية، تظهر حكومة بلا معارضة؛ حتى إذا ظهرت إلى الوجود عبر انتخابات وحيدة".

يتوقع كسنجر أن تتخذ الحكومات الجديدة التي تنتجها الثورات الرقمية في العقود القادمة شكل ائتلافات تتعلم الاستبداد، وسيكون ذلك ناجماً عن غياب القادة المتفردين الأقوياء أكثر منه عن عوامل التقانة. فمن دون وجود قائد مسيطر ورؤيا، ستكون مشاركة الحكومة للسلطة الخيار الأكثر قابلية للتطبيق؛ نظراً إلى كونه يرضي معظم المشاركين. إلا أن هذه الحكومات ستجازف دائماً بعدم تحقيق ما يكفي من التباين عن النظام السابق أو الجيل السابق من الفاعلين السياسيين.

ما الثورات سوى تجلٍّ للاستياء. وهي تبقى في الذاكرة لأنها غالباً ما تحمل نفحة رومانسية يسهل توظيفها في السرديات الإنسانية التي تتناول مواضيع الحرية والانعتاق وتقرير المصير. ومع توفر المزيد من التقانة تظهر قصص جديدة ذات عناوين جميلة تأسر خيالنا. فحتى حين يفشل الثوار نجدهم يحتلون في تاريخنا الجمعي مكانة خاصة تضفي عليهم الاحترام؛ وإن على مضض. فثمة مكونات في غاية الأهمية في التطور السياسي البشري تمثل جوهر مفهومنا عن المواطنة والعقد الاجتماعي، والجيل التالي من التقانات لن يغير شيئاً فيها.

وإذا كانت الثورات هي الطريقة التي يختارها البعض لتحقيق التغيير داخل النظام أو للتعبير عن استيائهم من الوضع القائم، فسيكون هناك دائماً أشخاص ومجموعات تسعى إلى تحقيق الغايات نفسها بوسائل أشد عنفاً وتدميراً. فالإرهابيون

والمتطرفون العنيفون سيشكلون دوماَ جزءاَ من مستقبلنا كما هم اليوم. سنتحرى في الفصل القادم مستنبتات التطرف في المستقبل، سواء أكانت في العالم المادي أم الافتراضي، وسنوضح كيف سيغير توسع ميدان المعركة طبيعة الإرهاب، والأدوات التي علينا أن نقاتل بها.

الفصل الخامس: مستقبل الإرهاب

كما وضحنا في ما سبق، تمكن التقانة من تحقيق المساواة في الفرص، فهي تمنح الناس أدوات يستخدمونها للغايات التي يرتأونها. وهي غايات بناءة رائعة أحياناً، لكنها قد تكون مدمرة على نحو لا يمكن تصوره في أحيان أخرى. ولا مفر من أن ينتفع الإرهابيون والمتطرفون العنيفون بدورهم من الاتصالات. فحين تنتشر الاتصالات، تنتشر معها المخاطر أيضاً. وستشتمل النشاطات الإرهابية في المستقبل، من التجنيد إلى التنفيذ، على جوانب مادية وافتراضية. فالمجموعات الإرهابية ستستمر في قتل الآلاف سنوياً، بالقنابل وغيرها من الوسائل. وهي أخبار سيئة بالنسبة إلى الجماهير، والدول التي لديها مسبقاً ما يكفي من المصاعب التي تواجهها في حماية بلادها في العالم المادي، والشركات التي يزداد تعرضها للخطر.

تبقى بالطبع إمكانية مرعبة، وهي أن تحوز إحدى هذه المجموعات أسلحة نووية أو كيميائية أو بيولوجية. ونتيجة اعتماد العالم المتقدم على تواصليته الخاصة (فجميع الأنظمة التي نعرفها تقريباً مرتبطة بشبكة افتراضية بطريقة ما)، سنكون في حالة ضعف قاتل أمام الإرهاب السايبري في أشكاله المختلفة. وهو ما ينطبق بالطبع على الأماكن الأقل اتصالاً، والتي تحدث فيها معظم الهجمات الإرهابية اليوم. وستنمو القدرات التقنية للمتطرفين العنيفين مع تطويرهم استراتيجيات التجنيد والتدريب والتنفيذ في العالم الافتراضي، ومع إدراكهم الكامل أن هجماتهم ستكون أكثر ظهوراً من أي وقت مضى بفضل التوسع المتزايد لشبكات الوسائط الاجتماعية العالمية.

لكن، بالرغم من هذه المكاسب التي سيحققها الإرهابيون، فإن تقانات الاتصالات ستجعلهم أقل حصانة من أي وقت مضى. فمقابل جميع الميزات التي يقدمها العيش في العالم الافتراضي للإرهابيين (خلايا صغيرة منتشرة في جميع أنحاء العالم، وصعوبة ملاحقة النشاطات التخريبية)، لا بد لهم من أن يعيشوا في العالم المادي أيضاً (لما يحتاجون إليه من مأكل ومسكن وفضاء مادي يستطيعون من خلاله استخدام هواتفهم وحواسبهم)، وهو بالضبط ما يجعلهم أضعف في العصر الرقمي الجديد. وسنستكشف في ما يلي كيف سيقسم الإرهابيون وقتهم بين العالمين، المادي والافتراضي، وكيف أنهم - على الرغم من تحقيقهم بعض المكاسب - سيرتكبون في النهاية المزيد من الأخطاء، وسيورطون المزيد من الأشخاص؛ مما يجعل مجال أعمال العنف أصعب بكثير.

مدى جديد ومخاطر جديدة

من المعروف جيداً أن الإنترنت قد تزود المجرمين والمتطرفين بمعلومات خطيرة، لكن ما نفهمه بدرجة أقل هو كيفية تطوّر ذلك على المستوى العالمي في المستقبل. فالكثير من الشعوب التي ستدخل عصر الإنترنت خلال العقد القادم شعوب فتية تعيش في مناطق مضطربة ذات فرص اقتصادية محدودة وتاريخ حافل

بالنـزاعات الداخلية والخارجية. لذا، إنّ دخول العصر الرقمي الجديد في بعض المناطق سيعني أيضاً زيادة في النشاطات العنيفة التي يغذيها توفر التقانة. وما انتشار أجهزة التفجير منـزلية الصنع سوى مؤشر قوي على أن هذه العملية قد بدأت بالفعل.

خلال تنقلنا في العراق عام 2009 صدمنا لما لاحظناه من سهولة ممارسة الإرهاب. فقد أخبرنا نقيبٌ في الجيش أن إحدى المخاوف العظيمة الموجودة لدى جميع القوات الأمريكية التي تسيّر الدوريات تتمثل في أجهزة التفجير المحسَّنة (آي.أي.دي) التي تزرع على قارعة الطريق. ففي الأيام الأولى للحرب كانت هذه الأجهزة مكلفةً في إنتاجها وتتطلب مواد خاصة، لكن أدوات صناعة القنابل وتعليمات إعدادها أصبحت مع الوقت متوفرةً على نطاقٍ واسع، ويمكن لأي متمرد محتمل الوصول إليها. وأجهزة عام 2009 كانت أرخص، وأكثر ابتكاراً، ومصممةً بطريقة تتفادى الإجراءات المضادة التي أصبحت معروفة، عبر تعديلاتٍ بسيطة عليها. حيث يتم لصق القنبلة مع صاعقها على هاتفٍ خلوي مجهز برجاج، حيث يمكن تفجيرها عن بعد عبر الاتصال برقم الهاتف (وسرعان ما رد الأمريكيون على هذا التكتيك بإدخال نظم التشويش التي تفصل الاتصالات النقالة ضمن نطاق محدود). والفعالية العنفية التي كانت ذات يوم معقدةً ومربحة (تدرّ على المتمردين آلاف الدولارات) أصبحت عمليةً مبتذلة اليوم يمكن لأي شخصٍ اللجوء إليها إذا امتلك الرغبة في المبادرة من دون أن تكلفه أكثر من ثمن بضع سجائر.

إذا كان تحضير متمرد لجهاز تفجير محسن يتم تفعيله كهربائياً بواسطة الهاتف النقال لا يزيد صعوبة اليوم عن مشروع علمي في المدرسة الثانوية، فماذا يمكننا أن نستنتج من ذلك حول المستقبل؟ هذه هي أحد المظاهر المشؤومة لما يسميه أندي روبن مبتكر أندرويد في التقانة، والتي غالباً ما يُحتفى بها خارج سياق الإرهاب. إذ يخبرنا روبن أنه "سيسهل على المواطنين أن يتحولوا هم أنفسهم إلى مصنعين عبر تجميع عناصر معدلة من منتجات اليوم لصنع شيءٍ كان بناؤه في السابق في غاية الصعوبة بالنسبة إلى مواطنٍ عادي". و الناشئة هذه تنتج في العالم عدداً غير مسبوق من الابتكارات العبقرية اليوم (وليست الطابعات ثلاثية الأبعاد سوى البداية). لكن ثمة - كما تدل معظم التطورات التقانية - جانب مظلم للابتكار.

أما أجهزة الإرهاب منـزلية الصنع في المستقبل، فغالباً ما ستجمع بين أجهزة التفجير المحسنة وألعاب الطائرات التي يمكن شراؤها على الشبكة أو من متجر ألعاب. والحوامات البسيطة ذات التحكم عن بعد متوفرةٌ منذ الآن بالفعل، فحوامة إي.آر.درون الرباعية التي صنعتها شركة باروت كانت إحدى الألعاب الأكثر مبيعاً في موسم الكرسمس عام 2011-2012. وهذه الألعاب مزودة بكاميرا، ويمكن قيادتها باستعمال هاتف ذكي. فتخيل نسخةً أكثر تعقيداً منها تستخدم اتصالات واي.فاي تقوم بتوليدها بنفسها، ويتم تزويدها بقنبلةٍ منـزلية الصنع تثبت على عجلات الهبوط لتنتج بذلك مستوى جديداً تماماً من الإرهاب المحلي المتاح في كل مكان. ولا شك في أن المعارف والموارد والمهارات التقنية التي يستلزمها إنتاج

مثل هذه الطائرات ستكون متوفرة في كل مكانٍ عملياً في المستقبل القريب. وستصبح إمكانية الملاحة المستقلة التي ناقشناها في ما سبق متوفرةً بشكلٍ عام، ويمكن دمجها على شريحة، مما سيسهل على الإرهابيين والمجرمين تنظيم هجوم باستخدام هذه الطائرات من دون تدخلهم. وسيكون تحسين القوة التدميرية في الهجومات المادية مجردِ جانبٍ من تأثير انتشار التقانة على الإرهاب العالمي. فالإرهاب السايبري أيضاً أحد هذه الجوانب بالطبع (والمصطلح نفسه يعود إلى ثمانينيات القرن العشرين)، وهو يشكل تهديداً لا ينفك يزداد خطورةً. ولأغراض هذا الكتاب، سنعرف الإرهاب السايبري على أنه القيام بهجومات ذات دوافع سياسية أو إيديولوجية، تستهدف المعلومات أو بيانات المستخدمين أو نظم الحاسب، بهدف تحقيق نتائج عنفية (ثمة بعض التراكب في التكتيكات بين الإرهاب السايبري والاختراق الإجرامي لكن التمييز بينهما يتم على أساس الدوافع بشكل عام).

من الصعب تخيل المجموعات المتطرفة التي تطلق عملياتها من كهوف تورا بورا وقد أصبحت تشكل تهديداً سايبرياً. لكن انتشار الاتصالات حول العالم سيسمح للأنحاء القصية أيضاً بالوصول إلى الشبكة وإلى الأجهزة النقالة المتطورة إلى حدٍّ لا بأس به. ولا مفر من افتراض أن هذه المجموعات ستمتلك المهارات التقنية اللازمة لشن الهجمات السايبرية. وهذه التغييرات، وحقيقة أن اتصالاتنا بحدّ ذاتها تمثل أهدافاً محتملة للمتطرفين لا تعد ولا تحصى، ليست تطورات مبشرة بالخير.

لنفكر في بعض الاحتمالات البسيطة. إذا نجح الإرهابيون السايبريون في اختراق شبكة أمنية لمصرف كبير، فستصبح جميع بيانات مستخدميه وأموالهم في خطر. (بل إن مجرد التبليغ عن التهديد القائم، في الظروف المناسبة، قد يسبب تهافتاً لسحب الودائع من المصرف). وإذا استهدف إرهابيون سايبريون نظام المواصلات في مدينة ما أو بيانات الشرطة أو سوق الأسهم المالية أو الشبكة الكهربائية، فيمكنهم تجميد آليات العمل اليومي للمدينة.

ستتكفل الدروع الأمنية لبعض المؤسسات والمدن بمنع ذلك، لكن مثل هذه الحماية لن تكون متوفرةً للجميع. فنيجيريا - التي تخوض معارك مع الإرهاب المحلي، وتعاني من ضعف مؤسساتها - أصبحت بالفعل زعيمة العالم في مجال الاحتيال على الإنترنت. فمع انتشار الاتصالات المتوفرة في مدن مثل لاغوس وأبوجا إلى الشمال الريفي الأكثر اضطراباً (حيث يسود التطرف العنيف)، سيتحول كثيرون إلى محتالين، وسيسهل انقيادهم وراء قضية مجموعة إسلامية عنيفة مثل بوكو حرام (النسخة النيجيرية من طالبان)، وستكفي مجموعة من المجندين الجدد لتحويل بوكو حرام من أخطر منظمة إرهابية في أفريقيا الغربية إلى أقوى منظمة إرهاب سايبري.

ليس من الضروري أن تنحصر هجمات الإرهاب السايبري باختراق النظام. فإرهابيو المخدرات وتجارها والمجرمون في أمريكا اللاتينية يتزعمون العالم في مجال الخطف. لكن الخطف التقليدي سيصبح أكثر مجازفة في المستقبل؛ نظراً إلى انتشار ظواهر مثل تحديد الموقع الجغرافي الدقيق باستعمال الهواتف النقالة (فحتى إذا دمر الخاطفون هاتف الرهينة، سيكون آخر مكانٍ تواجد فيه قد سجّل في

مكانٍ ما على السحابة. وسيلجأ الأفراد المدركون للحالة الأمنية في البلدان التي ينتشر فيها الخطف على الأرجح إلى اقتناء تقانة بحجم قلم قابلة للارتداء يقوم بالتبليغ عن موقعهم باستمرار وبالزمن الحقيقي. بل إن من هم في خطرٍ أكبر سيحملون أشكالاً من الإضافات الفيزيائية التي تحدثنا عنها سابقاً). من جهة أخرى، سيشيع الخطف السايبري؛ أي سرقة الهويات الشبكية للأثرياء أو أي شيءٍ آخر، (من تفاصيل حساباتهم المصرفية، إلى حسابات الشبكات الاجتماعية العامة التي يملكونها)، والمطالبة بمالٍ حقيقي فديةً للمعلومات. وبدلاً من الاحتفاظ بالرهائن سجناء في الأدغال، ستفضل عصابات القوات المسلحة الثورية الكولومبية مثلاً، أو المجموعات المشابهة، أخذ رهائن افتراضيًّا لما ينطوي عليه ذلك من قدرٍ أقل من المجازفة والمسؤولية.

تقدم الهجمات السايبرية ميزات واضحة للمجموعات المتطرفة؛ أي خطراً جسدياً ضئيلاً أو معدوماً على الأشخاص، وتوظيف الحد الأدنى من الموارد، وإمكانيات إلحاق أضرار هائلة. فستتسبب هذه الهجمات لضحاياها بضياع لا يصدق؛ لصعوبة تتبع مصادر الهجمات الافتراضية* كما نوهنا سابقاً. كما ستدخل الرعب إلى قلوب الجماهير الهائلة من الضحايا المحتملين (ويعد من بين هؤلاء كل شخص يعتمد عالمه على الاتصالات). إننا نعتقد أن الإرهابيين سينتقلون بعملياتهم أكثر فأكثر إلى الفضاء الافتراضي، بالترافق مع الهجمات في العالم المادي. وبينما ستبقى أسلحة الدمار الشامل مصدر الخوف الرئيس (خصوصاً مع كل هذه الثغرات في الحدود التي تجعل تهريب قنبلة بحجم حقيبة إلى البلاد أمراً سهلاً)، قد لا تشتمل نسخة المستقبل من أحداث الحادي عشر من أيلول على عمليات تفجير وخطف طائرات منسقة، بل على هجمات يتم تنسيقها بين العالمين الافتراضي والمادي بنسب مدمرة يتم تصميم كل منها لاستغلال نقاط ضعف معينة في أنظمتنا.

قد يبدأ هجوم على أمريكا بهجوم مضلل على الجانب الافتراضي، ربما على شكل هجوم واسع النطاق يستهدف نظام التحكم بالملاحة الجوية؛ يُعمد فيه إلى توجيه عدد كبير من الطائرات حيث تطير على ارتفاعاتٍ خاطئة أو تتخذ مسارات قد تؤدي إلى حدوث اصطدامات. وعندما يندلع الذعر، ربما سيُشنّ هجوم سايبري آخر يعطل قدرات الاتصالات في الكثير من أبراج التحكم بالمطارات محولاً الأنظار إلى السماء؛ إذ سيخشى الناس أن يكون هذا الهجوم الجوي هو الذي كانوا يخشونه. وفي هذه الأثناء، قد يأتي الهجوم الحقيقي من الأرض عبر ثلاث قنابل تم تهريبها عبر كندا تنفجر في الوقت نفسه في نيويورك وشيكاغو وسان فرانسيسكو. وبينما تتفرج بقية البلاد على ردود الفعل الأولى التي تحاول التصرف وتقدير الأضرار، قد تأتي موجة تالية من الهجمات السايبرية وتشلّ الشرطة وأقسام الإطفاء ونظم معلومات الطوارئ في هذه المدن. وإذا لم يكن ذلك مروعاً بما يكفي، وبينما تتباطأ عمليات الطوارئ المدنية المكبلة بالدمار المادي الهائل وفقدان الأرواح، يمكن لفيروسٍ حاسوبـي متطور أن يهاجم نظم التحكم الصناعية التي تشغِّل البنى التحتية الحيوية في أنحاء البلاد مثل الماء والطاقة والنفط وأنابيب الغاز. فالاستيلاء على هذه النظم، التي تدعى نظم التحكم الإشرافي وتحصيل

البيانات (سكادا)، سيمكن الإرهابيين من فعل أي شيء، كقطع شبكات الطاقة، وقلب اتجاه محطات معالجة مياه الصرف الصحي، وتعطيل نظم مراقبة الحرارة في محطات الطاقة النووية (عندما ضربت دودة ستاكس.نت المرافق النووية الإيرانية عام 2012 كان عملها يرتكز على اختراق عمليات التحكم الصناعية ضمن أجهزة الطرد النووية). ويبقى أن نؤكد أن تنفيذ هجومٍ على هذا المستوى سيكون صعباً إلى درجةٍ لا تصدق، بل لا يمكن تخيلها. فالاستيلاء على نظام سكادا واحد يتطلب معرفةً مفصلةً ببنيانه الداخلي، وشهوراً من البرمجة، ودقةً في التوقيت، لكن بعض أشكال الهجومات الفيزيائية والسايبرية المنسقة لا يمكن تجنبها.

قليلةٌ هي المجموعات الإرهابية التي ستمتلك المستوى المطلوب من المهارات أو التصميم لتنفيذ هجمات على هذا النطاق خلال العقود القادمة. بل إن نقاط الضعف التي تنتجها التقانة لديها ستؤدي إلى وجود عدد أقل من العقول المدبرة الإرهابية بشكل عام. لكن العقول التي ستكون موجودة بالفعل، ستكون أكثر خطورة بعد. فربما لن يكون تفوق المجموعات الإرهابية في المستقبل عائداً إلى استعداد أفرادها للموت من أجل قضيتها، وإنما إلى مدى تمكنها من التقانة.

ستكون منصات كثيرة عوناً للمجموعات المتطرفة تساعدها على التخطيط والتعبئة والتنفيذ والتجنيد؛ والأمر الأخير هو الأهم كما أشرنا سابقاً. فربما لا تكون هناك كهوف كثيرة على الشبكة، لكن تلك النقاط المظلمة التي تبرم فيها الصفقات الشريرة بأشكالها كافة؛ من المواقع الإباحية للأطفال إلى غرف المحادثة الإرهابية، ستبقى موجودةً في العالم الافتراضي. وستعمل المجموعات الإرهابية في المستقبل، حين تفكر في مستقبلها، على تطوير منصاتها الاجتماعية المتطورة والآمنة الخاصة بها، والتي ستلعب دور مخيمات التدريب الرقمية في النهاية. وستوسع هذه المواقع مداها ليصل إلى المجندين الجدد المحتملين، وستتمكن من تشارك المعلومات بين خلايا مختلفة، وستوفّر وسطاً أو ملتقى على الشبكة للأفراد ذوي الميول المشابهة. وستكون هذه البيوت الآمنة الافتراضية بالنسبة إلى المتطرفين هبةً لا تقدر بثمن؛ على افتراض عدم وجود عملاء مزدوجين وتوفر تشفير رقمي قوي بما يكفي. وستحاول وحدات مكافحة الإرهاب والسلطات التنفيذية والنشطاء المستقلون إغلاق هذه المواقع، أو اختراقها، لكنهم لن يتمكنوا من ذلك، فما من شيء أسهل من تغيير الموقع أو تغيير مفاتيح التشفير ضمن فضاء افتراضي لا حدود له حيث تبقى المنصات حيّة.

ستكون الحنكة في مجال وسائل الإعلام إحدى أهم سمات الإرهابيين العابرين للحدود في المستقبل. فعليها ستعتمد عمليات التجنيد وأشياء أخرى. وقد سبق لمعظم المنظمات الإرهابية أن وضعت قدمها في ميدان التسويق الإعلامي، وما كان يبدو سخيفاً ذات يوم (كموقع القاعدة المحشو بالتأثيرات الخاصة، أو حساب مجموعة شباب الصومال المتمردة على تويتر)، بدأ يتكشف عن واقعٍ جديد غريب. ولنا في قضية أنور العولقي ذائعة الصيت خير مثال. فقد كان العولقي رجل دينٍ متطرفاً مولوداً في أمريكا، انضم إلى القاعدة في اليمن، وكان حضوره القوي يعود بشكلٍ أساسي إلى ترويجه الذاتي لنفسه. حيث كان يستخدم مقاطع الفيديو

الفيروسية والشبكات الاجتماعية لينشر عظاته الكاريزماتية على المستوى الدولي. وكان للعولقي تأثير لا يمكن إنكاره بصفته أول إرهابيٍ كبير يحقق الإثارة على موقع يوتيوب (كانت كلماته تقتبس من قبل إرهابيين ناجحين أو جدد كما لو كانت مصدر إلهام لهم). وعادت عليه شهرته بمركزٍ على قائمة الحكومة الأمريكية للأهداف عالية القيمة، ليقتل في هجوم طائرة من غير طيار في أيلول عام 2011.

فحتى الشخصيات الدينية الأكثر عداءً للغرب في المملكة العربية السعودية تستخدم كلها التقانة، بل إن عدداً منهم يستخدم الأجهزة النقالة والشبكات الاجتماعية على نحوٍ متزايد لإصدار الفتاوى. ويعلم مراقبو الشرق الأوسط أن هذا يمثل تغييراً عميقاً، خصوصاً في المملكة العربية السعودية التي تُعرف فيها المؤسسة الدينية بالتباطؤ في تقبل التقانة. ولا يمكن لهذا التوجه سوى أن يستمر.

نظراً للأهمية التي سيتمتع بها التسويق الرقمي بالنسبة إلى الإرهابيين في المستقبل فإننا نتوقع أنهم سيسعون إلى اختراق شركات الهواتف النقالة والإنترنت أكثر فأكثر. وقد بدأت بعض المجموعات بالفعل بمحاولاتٍ مشابهة. فقد أخبرنا ماجد نواس، الزعيم السابق في حزب التحرير (وهو مجموعة متطرفة عالمية تسعى إلى قلب الحكومات في البلدان ذات الغالبية المسلمة عبر الانقلابات العسكرية وإنشاء دولة إسلامية عظمى على مستوى العالم) أن منظمته كانت تتبع سياسة تجنيدٍ بين صفوف العاملين في شركات الهواتف النقالة. "كنا نقيم أكشاكاً للدعاية أمام مكاتب موتورولا في باكستان، ثم نجحنا في تجنيد بعض العاملين في مكاتب موتورولا، فصاروا يسربون لنا أرقام محرري الصحيفة الوطنية في باكستان" يقول لنا. وبعدها، كان أعضاء حزب التحرير يمطرون هؤلاء المحررين برسائل نصية مليئة بالدعاية ونقاط المناقشة، بل والتهديدات أيضاً. وكان موظفو موتورولا، وفقاً لنواس، يقدمون لحزب التحرير مساعدات أكبر من هذه بعد، عبر إخفاء هويات أعضائه عندما يستعملون خدمة الهاتف لكتابة الرسائل النصية مما يسمح لهم بالعمل من دون اكتشافهم.

إذا لم تستهدف المجموعات المتطرفة شركات الاتصالات النقالة بذاتها فإنها ستجد طرقاً أخرى تحقق من خلالها السيطرة على منصاتها القوية. فمجموعاتٌ مثل حماس وحزب الله تعمد إلى كسب الدعم الشعبـي عبر تقديم خدماتٍ تمتنع الدولة عن تقديمها أو تعجز عن تقديمها بشكلٍ لائق. والخدمات والدعم والترفيه، جميعها تخدم في تقوية مصداقية المجموعة وولاء قاعدتها. إذ يمكن لحماس تطوير عائلةٍ من التطبيقات للهواتف الذكية الرخصية التي يستخدمها الجميع، والتي تقدم من خلالها كل شيء؛ من معلومات الرعاية الصحية إلى عمليات العملة النقالة، إلى ألعاب الأطفال. وسيتم بناء هذه المنصة التي لا تقدر بثمن وتشغيلها من قبل عناصر حماس والمتعاطفين معها، وحتى إذا قام موقع متجر آبل للتطبيقات بحجب تطبيقاتها بناءً على أمرٍ من الحكومة الأمريكية، أو إذا اتخذت الأمم المتحدة إجراء مشابهاً بحقها، فسيكون من الممكن بناء التطبيقات من دون أية صلةٍ رسمية بحماس، ثم ترويجها شفهياً. وسيكون لذلك أثر هائل على جيل الشباب.

مع ازدياد خطر المجموعات المتطرفة وقدراتها بفضل الاتصالات العالمية،

ستفقد الحلول التقليدية فعاليتها تدريجياً. ففي كثيرٍ من أنحاء العالم، سيكون الاكتفاء بسجن الإرهابيين غير ذي أثر على شبكتهم أو على قدرتهم على التأثير فيها. فالأجهزة المهربة ستسمح للمتطرفين بإقامة مراكز تحكمٍ وقيادة داخل جدران السجن. ولن تنفك مهمة مصادرة هذه الأجهزة، أو الحدّ من فعاليتها على الأقل، تزداد صعوبةً مع انخفاض حجم المكونات الأساسية للهواتف الذكية، من معالجات وبطاقات سيم (بطاقات الذاكرة المستخدمة في الهواتف النقالة، والقادرة على نقل البيانات من هاتف إلى آخر) وغيرها، وازدياد فعاليتها.

وقد بدأت هذه الممارسات بالفعل، وإن بطريقةٍ مضحكة في بعض الأحيان. ففي عام 2011 أوقف مسؤولو سجن كولومبـي فتاةً في الحادية عشرة من عمرها، كانت في طريقها لزيارة قريبٍ لها مسجونٍ في ميديلن، بسبب شكل سترتها الغريب، فوجدوا أنه تم إلصاق 72 هاتفاً نقالاً ومسدساً على ظهرها. وفي البرازيل، قام السجناء بتدريب حمامٍ زاجل على تهريب مكونات الهاتف جواً. وفي حالةٍ واحدة على الأقل، قامت عصابةٌ محلية بتكليف مراهقٍ بقذف الهواتف من فوق أسوار السجن بواسطة قوسٍ ونبال (وقبض على الولد عندما أصابت إحدى نباله ضابطاً في السجن).

لا يحدث هذا في العالم النامي فقط. فقد أخبرنا عضوٌ سابق في عصابةٍ في جنوب لوس أنجلوس أن السعر الشائع اليوم لهاتفٍ ذكي مهرب في السجون الأمريكية يبلغ نحو ألف دولار. حتى إنه من الممكن الحصول على الحواسب اللوحية مقابل السعر المناسب. وتابع شرحه مبيناً كيف تمكن هذه الأجهزة نـزلاء السجن الذين يتمتعون باتصالاتٍ جيدة من إدارة أعمالهم المحظورة، وتنسيقها من خلف القضبان عبر منصات الشبكات الاجتماعية الشائعة. ففي العام 2010، عندما أضرب سجناءٌ في ستة سجونٍ على الأقل في ولاية جورجيا الأمريكية في الوقت نفسه احتجاجاً على ظروف سجنهم، تم تنظيم احتجاجهم بشكلٍ شبه كامل بواسطة شبكةٍ من الأجهزة النقالة المهربّة.

تأتينا أفضل الأمثلة (وأنجحها) على النشاطات التي تنفذ داخل السجن من أفغانستان، البلد ذي معدلات الاتصالات الأدنى في العالم. فسجن بلشرخي الواقع في ضواحي كابول هو أضخم السجون في البلاد وأسوأها سمعة. وفي هذا السجن، الذي شُرعَ في بنائه في سبعينيات القرن الماضي، واكتمل في حقبة الاحتلال السوفييتي، كان عشرات الآلاف من المساجين السياسيين يُقتلون في السنوات الأولى كل عام، وكان كثيرون منهم يخضعون للتعذيب عقوبةً لهم على ميولهم المعادية للشيوعية. وعاد السجن ليكون تحت الأضواء خلال الاحتلال الأمريكي بصفته المركز العصبـي للإرهابيين. فبعد تمردٍ عنيف في زنازين الجناح الثالث عام 2، اكتشفت السلطات الأفغانية خليةً (بما للكلمة من معنيين) إرهابية بكامل نشاطها كان النـزلاء يستخدمونها لتنسيق هجماتٍ قاتلة خارج جدران السجن. وكان الباب الخلفي للخلية مغطىً بأسلاكٍ كهربائية حيّة ملفوفة حول القضبان كالدوالي مصدرةً وهجاً أحمر خفيفاً في الممر، بينما كانت الجدران مزينةً بالسيوف والآيات القرآنية. وكان مساجين طالبان والقاعدة قد استولوا قبل ذلك بسنوات على جناح الزنازين

الثالث، وعن طريق التهريب الفعال للهواتف وأجهزة الراديو، وتجنيد أفراد ضالعين من ضمن نـزلاء السجن، وتهديد الحراس وعائلاتهم، حوّل هؤلاء النـزلاء المتطرفون بيئتهم إلى سجنٍ من دون جدران (ليكون مربضاً آمناً يحميهم من الطائرات غير المأهولة وغيرها من الأخطار) يستطيعون انطلاقاً منه توسيع منظمتهم، وتنفيذ مخططات الابتزاز، وتنسيق الهجمات الإرهابية في مدينةٍ تبعد عنهم عشرين ميلاً. فكانوا يجندون اللصوص الحقيرين ومدمني الهرويين والمسيحيين (أي النـزلاء الذين جعلتهم منـزلتهم المحتقرة في المجتمع الأفغاني صيداً يسيراً للتطرف) عن طريق المال أو التهديد بالعنف.

بعد تمرد عام 2008 ساد اعتقادٌ بأن إعادة توزيع هؤلاء النـزلاء على أجنحة مختلفة قد أنهى شبكتهم الإرهابية، أو عطلّ إلى حدٍّ كبير قدرتها على العمل على الأقل. إلا أنه لم يمض عامان حتى اعترف مسؤولو السجن بعد سلسلة هجماتٍ في كابول بأن الخلية قد أعادت تشكيل نفسها داخل السجن مباشرةً تقريباً، وأن محاولات السلطات للحد من قدراتها العملياتية عبر التشويش المتقطع (حيث لا يمكنها الاستفادة من الهواتف النقالة المهربة) قد فشلت في معظمها. وكان سجن بلشرخي مأوى لكثيرٍ من النـزلاء ذوي القيمة العالية بالنسبة إلى أفغانستان، وكان الجيش الأفغاني يديره مع مستشارين أمريكيين، إلا أن أحداً من هؤلاء لم يبد قادراً على التحكم بشبكات الهاتف النقال. وعندما رافق جيريد المبعوث الخاص السابق إلى أفغانستان ريتشارد هولبروك في رحلةٍ إلى كابول، زار السجن، وقابل أحد قادة تمرد الجناح الثالث السابقين الذي كان لا يزال مقيماً في السجن، وهو قائدٌ متطرف اسمه ملا أكبر آجي، لكي يقدّر مدى تغير الظروف في السجن بعد عملية قمع التمرد، وحين طلب منه مازحاً رقم هاتفه، لم يكن من آجي سوى أن دس يده في ردائه مخرجاً هاتفاً حديثاً ليدون بفخرٍ اسمه ورقم هاتفه على قصاصةٍ ورقية: 070-703-1073.

تبينُ تجربة بلشرخي الأخطار التي ينطوي عليها الجمع بين العصابات والمتطرفين وتجار المخدرات والمجرمين في السجون خلال العصر الرقمي. فخارج جدران السجن، تتراكب هذه الشبكات المختلفة أحياناً وتستخدم المنصات التقانية نفسها، لكنها حين توضع على مقربةٍ من بعضها داخل السجون، وبمساعدة الأجهزة المهربة، قد تتحول إلى عُقدٍ موحدة خطيرة. فقد يقوم تجار مخدرات من جماعةٍ مكسيكية بتبادل معلوماتٍ قيمة حول شبكات تهريب الأسلحة العابرة للحدود مع متطرفين مقابل المال أو مقابل منح العصابة موطئ قدم في سوقٍ جديدة. وعندما يصل الطرفان إلى اتفاق يتبادلان من خلاله المنفعة، يمكن لكلٍ منهما استخدام الهاتف النقال لإعلام منظمته باتفاق التعاون الجديد. وسيكون اعتراض الصفقات التي تُعقَد في السجن ويُتابَع تنفيذها في المجتمع المفتوح صعباً، لأن صعوبة وضع جميع النـزلاء في زنازين انفرادية (وهو حلٌ غير واقعي) أو إغلاق تجارة الأجهزة المهربة (وهذا أيضاً غير وارد على الرغم من الجهود الهائلة) ستحدّ من نجاح سلطات السجن في منع حالاتٍ مثل هذه من الحدوث.

فإذا افترضنا أن شبكات التهريب في السجون ستتفوق بشكلٍ عام في ذكائها

على المسؤولين عن تعطيلها، وأن الطلب على الهواتف النقالة سيبقى مرتفعاَ بين نـزلاء السجون، فما هي الخيارات المتبقية لمنع سيناريو بلشرخي من الحدوث في مكانٍ آخر؟ إن أبسط الحلول هو أن يتم قطع الشبكة والتشويش عليها، حيث تصبح الهواتف المهربة بين أيدي نـزلاء السجن مجرد منصاتٍ مكلفة للعب ليس أكثر. لكن، من المنطقي أيضاً أن يكتشف شخص ما طريقةً لتجاوز هذا الحاجز. وإذا كانت الحمامات الحيّة لا تنفع، فقد تنفع الطائرات (الألعاب) الصغيرة المصممة على شكل حمامات، والقادرة على العمل كمحطات واي فاي نقالة.

ثمة خيار آخر يتمثل بمراقبة السلطة التنفيذية للفعاليات النقالة للمساجين وإيقافها. فالمعلومات الاستخباراتية المجموعة عبر التنصت على السحابة، وأشياء أخرى، سلطت الضوء على طريقة عمل الشبكات المحظورة. وثمة حلٌ أكثر تخريباً، وهو الدخول عمداً إلى الشبكات المهربة، عبر إيصال أجهزة إلى أيدي المساجين تكون مليئةً بالأفخاخ لتقوم تلقائياً بتسليم المعلومات، يمكن تصميم هذه الهواتف حيث تشي بالأسرار بسهولة من دون معرفة النـزلاء. وقد يثبت مع الوقت أن هذه الطريقة أنجع من تجنيد المخبرين من البشر وأكثر أمناً أيضاً.

ستحرص بعض المجتمعات على عدم ظهور السجين على الإنترنت وعلى اختفائه منها تماماً حين يكون وراء القضبان. وسيتم تجميد هويته الافتراضية بأمرٍ من المحكمة، وستمنع القوانين أي شخصٍ من محاولة التواصل معه، أو الاتصال به، أو حتى الترويج لحسابه المجمد. وما إن يطلق سراحه، حتى يطلب منه تزويد الضابط المسؤول عنه في فترة الاختبار بمفاتيح الوصول إلى حساباته على الشبكة. فالبديل الذي سيعتمد في العصر الرقمي لأصفاد القدمين عبارة عن برمجيات تضعها الحكومة لتتبع النشاطات على الشبكة وتقييدها. ولن ينحصر ذلك في الحالات الواضحة فقط، مثل المتحرشين بالأطفال (الذين يتم تقييد نشاطاتهم على الإنترنت كشرطٍ من شروط فترة الاختبار)، بل سيطبق على جميع المجرمين المدانين خلال فترة اختبارهم*. يمكن منع شخصٍ يستخدم معلومات يتيحها له منصبه لغاياتٍ خاصة بمنعه مؤقتاً من ممارسة جميع أشكال التجارة الإلكترونية. فيمنع من الاتجار على الإنترنت، ومن خدمات الصيرفة الشبكية، ومن شراء السلع على الإنترنت. أما الشخص الذي يكون قد صدر بحقه أمر تحفظي، فقد يمنع من زيارة صفحات الشخص المهدد على الشبكات الاجتماعية أو البحث عنه بالاسم على الشبكة، أو زيارة صفحات أصدقائه أيضاً.

لكن الكثير من الحلول سيتم للأسف التحايل عليها في عصر الإرهاب السايبري مع تمكن الكثير من المجرمين من العمل متخفين.

صعود المخترقين الإرهابيين

يعتمد مقدار الخطر الذي يمثله الإرهاب السايبري بالنسبة إلى شخص ما على نظرته إلى الاختراق. فالبعض لا يزال يحتفظ بصورة المخترق المراهق المقيم في قبو، والذي يسيطر على أنظمة الهاتف من باب المرح. لكن القرصنة تطورت تطوراً كبيراً خلال العقد الأخير، وتحولت من هواية إلى نشاط رئيس مثير للجدل.

فظهور الناشطين المخترقين (الهاكتيفيست، أي المخترقون الذين تحرضهم دوافع سياسية أو اجتماعية)، ومجموعات مثل أنونيموس للاختراق التعاوني، يشير إلى نضوج في الرسالة والمنهج، ويبين ما يمكننا أن نتوقعه في السنوات القادمة. فالمخترقون يجدون باستمرار طرقاً جديدة لتنظيم أنفسهم بناءً على قضايا مشتركة. وسينظمون هجمات متطورة على أي شخص يعتبرونه هدفاً مناسباً ليشهروا بعد ذلك أخبار نجاحاتهم على الملأ. وستتطلب هذه المجموعات دائماً يقظة الحكومات والمؤسسات التي تهاجمها. وقد يتوجب أخذ تهديداتها بجدية أكبر مما يعتقد المرء؛ كما تبين النشاطات التي نراها اليوم، والتي تبدو أقرب إلى الاستعراضات البهلوانية. ولنا في قصة ويكيليكس، موقع نشر الأسرار الذي ناقشناه في ما سبق، وحلفائه من المخترقين المؤيدين له، خير مثال على ذلك.

أثار اعتقال مؤسس ويكيليكس، جوليان أسانج، في كانون الأول من عام 2010، عاصفةً من الغضب حول العالم، وخصوصاً بين الناشطين والمخترقين وخبراء الحاسب الذين كانوا يعتقدون أن هناك دوافع سياسية خلف تهم الاعتداء الجنسي التي وجهت إليه. وسرعان ما أدت سلسلة من الهجمات السايبرية إلى شل مواقع تابعة لأمازون كانت قد أوقفت استخدام ويكيليكس لمخدماتها، ومواقع أخرى كماستر كارد وباي.بال اللذين قاما بوقف جمع التبرعات لويكيليكس.

وتم تنسيق الحملة التي حملت رسمياً اسم من قبل منظمة أنونيموس، وهي جماعةٌ مرنة الترابط من المخترقين والناشطين، مسؤولةٌ عن سلسلة من هجمات حجب الخدمة الشهيرة التي استهدفت الكنسية السينتولوجية وأهدافاً أخرى. وقد تعهدت المجموعة خلال العملية بالثأر من أية منظمة اتخذت موقفاً ضد ويكيليكس. "مع أنه لا يربطنا الكثير بويكيليكس، إلاّ أننا نناضل للغايات نفسها. فنحن نريد الشفافية، ونقف في وجه الرقابة. ومحاولات فرض الصمت على ويكيليكس خطوات كبيرة باتجاه عالم لا يمكننا فيه قول ما نفكر فيه، ولا نستطيع فيه التعبير عن آرائنا وأفكارنا، ولا يمكننا أن ندع ذلك يحدث... وهو ما يدفعنا إلى تسخير مواردنا لزيادة الوعي، ولمهاجمة أولئك الذين يقفون ضد وصولنا إلى عالم الحرية والديموقراطية، ولدعم أولئك الذين يساعدوننا في الوصول إليه". سرعان ما عادت المواقع التجارية إلى العمل خلال بضع ساعات، لكن تعطيلها كان شاملاً، وربما أثر على ملايين المستخدمين الذين ليست لدى معظمهم كزبائن أدنى فكرة أصلاً عن الضعف الذي تعاني منه هذه المواقع. بعبارةٍ أخرى، إن الناشطين المخترقين قد حققوا غايتهم، وأدت سلسلة من التحقيقات الدولية بعد ذلك إلى اعتقال العشرات من المشاركين المشتبه بهم من هولندا وتركيا والولايات المتحدة وإسبانيا وسويسرا ودولٍ أخرى.

ليست ويكيليكس أو أي من المجموعات الشبيهة بأنونيموس منظماتٍ إرهابية، مع أن البعض قد يدعي أن المخترقين الذين ينخرطون في فعالياتٍ مثل سرقة معلوماتٍ شخصية وسرية ونشرها على الشبكة قد يكونون كذلك. فالمعلومات التي يتم نشرها على ويكيليكس تعرض حياة الناس للخطر وتتسبب بأضرار دبلوماسية جسيمة*. وهنا بيت القصيد، فأياً كانت الخطوط التي تميز بين المخترقين غير

المؤذين وأولئك الخطرين (أو بين المخترقين والإرهابيين السايبريين في هذه الحالة)، فإنها لم تزدد سوى غشاوة في حقبة ما بعد أحداث الحادي عشر من أيلول. والتعاونيات اللامركزية، مثل أنونيموس، تبين بوضوح أن مجموعةً من الأشخاص ذوي الإرادة الذين لا يعرفون بعضهم بعضاً، ولم يسبق لهم أن التقوا، يمكنهم تنظيم أنفسهم حيث يصبح لديهم تأثير حقيقي في الفضاء الافتراضي. بل إنه ما من حاجةٍ إلى تظافر الجهود، حيث يمكن لفردٍ يتمتع بالبراعة التقنية (كالمهارة في هندسة الحاسب على سبيل المثال) أن يسيطر على آلاف الآلات لتنفيذ عرضه. فماذا سيحدث في المستقبل عندما تكثر هذه المجموعات؟ هل ستحارب جميعها من أجل حرية التعبير؟ إن الأمثلة التي برزت مؤخراً تبين أن علينا أن نتحضر لإمكانيات أخرى.

في العام 2011 كان العالم على موعدٍ مع مهندس برمجيات إيراني في الحادية والعشرين من عمره، كان يعمل على ما يبدو من طهران، ويسمي نفسه كومودو هاكر. وكان شخصاً غير اعتيادي مقارنةً بالناشطين المخترقين الذين يواجهون عادةً سيطرة الحكومة على الإنترنت. فقد أخبر نيويورك تايمز عبر البريد الإلكتروني أنه يرى أنه يتوجب على بلاده "أن تسيطر على غوغل وسكايب وياهو وغيرها". وكان واضحاً أن في نيته العمل على مكافحة المعارضين للحكومة داخل إيران. قال:"إنني أقوم بكسر جميع خوارزميات التشفير، لأمنح بلادي القدرة على السيطرة عليها جميعاً".

بعيداً عن المباهاة، تمكن القرصان كومودو من تزوير أكثر من خمسمئة شهادة ثقة على الإنترنت؛ ممّا مكّنه من تجاوز عمليات التحقق التي تجريها ، ومن الوصول إلى معلومات شخصية أو سرية للمستهدَفين من غير علمهم. ويقدر عدد الإيرانيين الغافلين الذين تم اختراق اتصالاتهم عبر عملياته بنحو 300 ألف خلال فصل الصيف. كما استهدف أيضاً شركات من المعروف أن المعارضين الإيرانيين يستخدمون منتجاتها (مثل غوغل وسكايب)، وشركات أخرى تتمتع بأهمية رمزية خاصة. حيث يقول إنه استهدف الشركة الهولندية ديجينوتار لأن قوات حفظ السلام الهولندية فشلت في حماية المسلمين البوسنيين في سربرنيتشا في العام 1995.

ولم تمض أشهر على الحملة البارزة التي شنها المخترق كومودو حتى ظهر ناشط قرصان إيديولوجي آخر من الشرق الأوسط أطلق على نفسه اسم أو.أكس.عمر، وأعلن أنه من "أشد كارهي إسرائيل"، وأنه يريد "القضاء على إسرائيل إلكترونياً". وفي كانون الأول من عام 2012، نجح في اختراق موقع وب رياضي إسرائيلي معروف، وبدأ بتوجيه زواره إلى موقع آخر يستطيعون منه تحميل ملف يحتوي على 400,000 رقم بطاقة ائتمانية (معظمها مكرر، لكن العدد الإجمالي لحَمَلة البطاقات المتضررين بالاختراق كان يقارب 20,000). وادعى أنه سيكون من الممتع مشاهدة 400,000 إسرائيلي يقفون في طوابير أمام البنوك وشركات بطاقات الائتمان... [و][و][و] مشاهدة البطاقات الإسرائيلية وهي ترفض في أنحاء العالم؛ مثلها مثل البطاقات النيجيرية". وبعد ذلك بأسابيع، عندما توقفت مواقع خطوط طيران العال الإسرائيلية وسوق الأسهم المالية نتيجة هجمات حجب خدمة

استهدفتها، صرح أو.أكس.عمر لأحد المراسلين أنه شكّل فريقاً مع مجموعة من المخترقين المناصرين للقضية الفلسطينية تُسمى نايتمير (الكابوس)، وأنهم سيخففون من الهجمات إذا اعتذرت إسرائيل عن الإبادة التي ارتكبتها بحق الفلسطينيين. وصرح نائب وزير الخارجية الإسرائيلي داني إيالون أنه يعتبر استهدافه "من قبل إرهابيين سايبريين وسام شرف". وقد أكد لاحقاً الاعتداءات على صفحته على الفيسبوك، لكنه أضاف أن المهاجمين "لن يجبرونا على الصمت، لا على الإنترنت ولا في أي منتدى آخر". فهل كان المخترق كومودو مهندساً إيرانياً شاباً حقاً؟ وهل ينسق أو.أكس.عمر حقاً مع مجموعة أخرى لشن هجماته؟ وهل كان أولئك المخترقون أفراداً، أم إنهم في الحقيقة عبارة عن مجموعات؟ هل من الممكن أن تكون إحدى هاتين الشخصيتين - أو كلتاهما - صنيعة دول تحاول استعراض قواها الرقمية؟ ثمة عدد غير محدود من السيناريوهات المحتملة، وهنا يكمن التحدي الذي يفرضه الإرهاب السايبري في المستقبل.

نظراً لصعوبة التحقق من مصادر الهجمات السايبرية، تضمحل قدرة المستهدَفين على الرد بالطريقة المناسبة بغض النظر عمن يدعي مسؤوليته عن تلك الهجمات؛ وهذا تشويش يضيف بعداً جديداً لحملات التضليل. وما من شك في أن ذلك سيستغلّ من قِبل الدول والأفراد على حدٍّ سواء، لذا سيصعب علينا في المستقبل أن نعرف مع من أو مع ماذا نتعامل.

لا يكفي الوصول المفاجئ إلى التقانة بمفرده لتمكين الأفراد المتطرفين من التحول إلى إرهابيين سايبريين. فثمة حاجز لا يزال إلى يومنا هذا يلجم تكاثر المخترقين الإرهابيين؛ ألا وهو المهارات التقنية. لكننا نتوقع أن يفقد هذا الحاجز أهميته مع انتشار الاتصالات، ووصول الأجهزة الرخيصة إلى الأماكن القصية، مثل منطقة الحدود الأفغانية الباكستانية والساحل الأفريقي والمثلث الحدودي في أمريكا اللاتينية (بين الباراغواي والأرجنتين والبرازيل). فالمخترقون في البلدان النامية يكونون عادة ممن علّموا أنفسهم بأنفسهم. وبما أننا نفترض أن توزع الشباب ذوي المواهب التقنية متساوٍ في كل مكان، فإن القراصنة المحتملين سيتمكنون، مع توفر الوقت والتقانة، من تحصيل المعلومات اللازمة لشحذ مهاراتهم. وسيكون من بين النتائج المترتبة على ذلك ظهور طبقة من الجنود الافتراضيين المستعدين للتطوع.

إذا كنا اليوم نرى مسلمين من الطبقة الوسطى التي تعيش في أوروبا يتوجهون إلى أفغانستان للخضوع للتدريبات في المعسكرات، فإننا قد نشهد العكس في المستقبل، أي أن يتوجه الأفغانيون والباكستانيون إلى أوروبا للتتلمذ على أيدي السايبريين. وعلى خلاف معسكرات التدريب، وما فيها من حقول الرماية وأجهزة اللياقة ومسارات الحواجز، قد لا تتعدى معسكرات التدريب الهندسية أن تكون بضع غرف مزودة ببعض الحواسب المحمولة التي تديرها مجموعة من طلاب الدراسات المؤهلين والساخطين، في لندن أو باريس. وإذا كان من الممكن التعرف على معسكرات التدريب اليوم في معظم الأحيان عبر الأقمار الصناعية، فإن معسكرات التدريب السايبرية سيتعذر تمييزها عن مقاهي الإنترنت.

ستسعى المجموعات والحكومات على حدٍّ سواء إلى تجنيد المهندسين والمخترقين لكي يحاربوا إلى جانبها. فحين تدرك كم يمكن لفريق من الاستراتيجيين ذوي المهارات التقنية تحسين قدراتها التدميرية، ستضاعف من بحثها عن المهندسين والطلبة والمبرمجين والمعلوماتيين في الجامعات والشركات لبناء الجيل التالي من الجهاديين السايبريين. ومع صعوبة إقناع أحدهم بأن يصبح إرهابياً، نظراً للتبعات المادية والقانونية، ستبقى الإيديولوجيا والمال والابتزاز أدوات هامة تستخدم في عملية التجنيد. وعلى خلاف الحكومات، يمكن للمجموعات الإرهابية أن تلعب ورقة معاداة المؤسسات التي قد تدعم قضيتها في أوساط بعض الشباب والفئات الساخطة من المخترقين. وستكون بالطبع لقرار التحول إلى إرهابـي سايبري في معظم الأحوال عواقب أقل على سلامة الشخص المعني.

ستلعب الثقافة دوراً هاماً في تحديد الأماكن التي ستتطور فيها جيوب الإرهاب السايبري هذه. فلطالما كانت الشعوب ذات الطابع الديني العميق، والتي تتواجد فيها عناصر متطرفة واضحة، أرضاً خصبة تقليدياً للتجنيد. وسينطبق ذلك على تجنيد الإرهابيين السايبريين أيضاً، وخصوصاً مع دخول أجزاء العالم الفقيرة بالاتصالات عصرَ الإنترنت. وتتحدد تجربة المستخدمين على الإنترنت إلى حدٍّ كبير بشبكاتهم القائمة، وبالبيئة الوسيطة التي يعيشون فيها. فلا يمكننا توقع تغير اجتماعي جذري بمجرد دخول الاتصالات. لكن ما سنشهده عوضاً عن ذلك هو تطور المزيد من قنوات الاتصال، والمزيد من المشاركة، والمزيد من الشخصيات الاحتيالية على الإنترنت.

بالطبع، هناك دولٌ داعمة للإرهاب ستسعى إلى تدبير هجماتٍ لا يمكن تعقبها، وإيران تسرب الأسلحة والأموال والتجهيزات لمجموعاتٍ مثل حزب الله وحماس والجهاد الإسلامي الفلسطينية وكتائب شهداء الأقصى والعديد من المجموعات المتطرفة في العراق. لكن محاولات الإرهاب السايبري بدأت تبدو أذكى ثمراً، لذا ستعمل إيران على تطوير قدراتها الافتراضية لوكلائها بما يتناسب مع ذلك، بمعنى أنها سترسل حواسب وتجهيزات شبكية وحزماً أمنية وبرمجيات ذات صلة، لكن ذلك قد يعني أيضاً تقديم التدريب الشخصي. فمن الوارد جداً أن تبدأ الجامعات التقنية باستقبال مبرمجين شيعة لبنانيين لتحقيق غايةٍ محددة هي دمجهم في جيش حزب الله السايبري الناشئ. وربما ترسل إليهم أغلى أدوات التشفير وتجهيزاته، أو قد تمول المدارس التقنية في معاقل حزب الله كالضاحية وبعلبك وجنوب لبنان لإنتاج حاضناتٍ يتدرب فيها المهندسون الواعدون لشن الهجمات السايبرية ضد إسرائيل. وربما تُستبدل سياسة تزويد رجال الأعمال الشيعة في البرازيل بالمال اللازم للشروع بالأعمال التجارية (وهذا تكتيك معروف للحكومة الإيرانية)، بتزويدهم بحواسب لوحية وأجهزة نقالة تحمل برمجياتٍ مخصصة.

لكن، يجب على أي نظام أو مجموعة إرهابية تجنّد مثل هؤلاء القراصنة أن تدخل في حساباتها وجود قدرٍ معين من المجازفة. فإذا لم يكن جميع المجندين من الشباب، فإن نسبةً لا يستهان بها منهم ستكون كذلك، وليس لأسبابٍ ديموغرافية فقط، فلطالما اعتقد علماء الاجتماع بوجود عوامل تطورية معينة تجعل الشباب

أكثر قابلية للتطرف (ثمة مناقشاتٌ كبيرة حول ماهية هذه العوامل بدقة، فالبعض يعتقدون أن لها علاقةً بكيمياء الدماغ، بينما يردها آخرون إلى عناصر سوسيولوجية في المجتمع بشكلٍ رئيس). أي إن الباحثين عن متطوعين لن تواجههم فقط مسألة تنظيم القراصنة الذين يُبدون مقاومةً خاصة للتنظيم الرسمي، بل عليهم أيضاً أن يتعاملوا مع مراهقين. وكما سنناقش في ما يلي، إن المشاركة في شبكة إرهابٍ افتراضي ستتطلب انضباطاً غير اعتيادي؛ وهذا الانضباط ليس سمةً مألوفةً بين المراهقين. فالأشياء التي تجذب معظم الشباب وتغريهم تبقى واحدة؛ كالتمتع بالاهتمام، والمغامرة، وإثبات الذات، والانتماء، والمركز. لذا، من شأن خطأ واحد أو تباه عرضيّ واحد على الشبكة يقوم به مخترق مراهق (أو شخصٌ ما يعرفه) أن يدمر الشبكة الإرهابية برمتها.

تماماً كما تعتمد عمليات مكافحة الإرهاب اليوم على مشاركة المعلومات الاستخباراتية والتعاون العسكري (كما يحصل بين الولايات المتحدة وحلفائها في جنوب آسيا)، فإن هذا الدعم المتبادل سيشتمل في المستقبل على مكونٍ افتراضي بلا شك. وبما أن الكثير من البلدان الأكثر تطرفاً ستكون من بين البلدان الأخيرة التي تصل إلى الإنترنت، فإنها ستحتاج إلى دعمٍ خارجي لتتعلم تصيّد الإرهابيين على الشبكة، وكيفية استخدام الأدوات التي أتيحت لها حديثاً. يجمع المتعهدون الكبار الثروات اليوم عبر المساعدة العسكرية الخارجية؛ لكن مع إضافة مكوناتٍ أمنية سايبرية إلى جهود التعاون الثنائي، ستظهر شركات أمنٍ حاسوبـي جديدة وقديمة لتستفيد بالمثل.

وستتغير السياسات العسكرية بدورها رداً على التهديدات التي يفرضها الإرهابيون السايبريون. فمعظم الإرهابيين الذين يلاحقهم الجيش اليوم يعيشون في دولٍ فاشلة، وفي مناطق لا حكم فيها. أما في المستقبل، فستصبح هذه الملاذات المادية الآمنة مترابطةً في ما بينها أيضاً؛ بما يسمح للإرهابيين بارتكاب الشرور افتراضياً من دون الخوف من سلطةٍ تنفيذية. وعندما تكشف الاستخبارات عن تخطيط إرهابيين سايبريين معروفين لشيءٍ خطير، فسيتم التفكير باتخاذ إجراءات مشددة، كتوجيه ضربات باستخدام الطيارات من دون طيار.

ستحاول الحكومات الغربية اجتذاب المخترقين المهرة ليقفوا إلى جانبها أيضاً. بل إن المخترقين يتعاونون مع الوكالات الحكومية في الولايات المتحدة اليوم بالفعل، على الأقل في ما يتعلق بالأمن السايبري. فعلى مدى سنوات، لم تنفك وكالات مثل وكالة مشاريع أبحاث الدفاع المتقدمة التابعة للبنتاغون (داربا) ووكالة الأمن القومي (أن.أس إي) توظف أفراداً موهوبين خلال مناسباتٍ معينة، مثل سلسلة مؤتمرات الأمن الحاسوبـي بلاك هات، وملتقى المخترقين في ديث كون. فقد أعلنت داربا عام 2011 عن برنامج جديد يدعى المسار السايبري السريع (سي.أف.تي) أسسه مخترق سابق تحول إلى مدير مشاريع لدى داربا، على أمل تسريع التعاون بين هذه الأوساط وتنسيقه. ومن خلال البرنامج بدأت داربا بمنح عقود قصيرة الأمد لأفراد وشركات صغيرة لكي تركز على مشاريع أمن شبكي محددة، وتميزت هذه المبادرة بتركيزها على اللاعبين الصغار والعاملين الأفراد بدلاً

من التركيز على الشركات الكبرى، وبقدرتها على تأمين الضوء الأخضر للمنح بسرعة، حيث وافقت داربا على ثمانية عقود خلال الشهرين الأولين من البرنامج (أو بسرعة الضوء، إذا جاز التعبير، إذا ما قورنت بالوتيرة الاعتيادية للتعاقد الحكومي). وقد سمحت هذه العملية لمجموعاتٍ تتمتع بمهاراتٍ لا يستهان بها - ما كانت لولا ذلك لتعمل مع الحكومة أو لصالحها - بالمساهمة بعمل هام لتحسين الأمن السايبري، بسهولة، وضمن الإطار الزمني الذي يعكس الطبيعة الفورية للعمل. وجاء البرنامج كجزءٍ من التحول الذي تشهده الوكالة باتجاه "الابتكار الديموقراطي المعتمد على الجماهير" والذي كانت بطلته ريجينا دوغان.

سألنا دوغان عن الدافع وراء هذا الأسلوب غير التقليدي في التعامل مع المسألة، فكثيرون سيدهشون لرؤية الحكومة وهي تدعو القراصنة إلى عقر دارها لمعالجة مشكلات أمنية حساسة. تقول دوغان: "ثمة فكرة منتشرة لدى كثيرين بأن القراصنة ومجموعة أنونيموس مجرد أشرار، لكن ما أدركناه، وما حاولنا إقناع آخرين به، هو أن القرصنة صفة تتطلب الموهبة. وأولئك الذين يكتسبون هذه الصفة (سواء أأطلقوها على أنفسهم أم أطلقها غيرهم عليهم) يمتلكون شيئاً هاماً يستطيعون المساهمة به في مسألة الأمن السايبري؛ وفقاً لطريقة تناولهم للمشكلات، والجداول الزمنية التي يعالجونها وفقها، وقدرتهم على التنفيذ والتحدي". وتضيف أن "نجاح المسار السايبري السريع كان إشارة إلى قابلية هذا النموذج للاستمرار. وأنا لا أعتقد أن علينا الاكتفاء بهذا النموذج فقط، بل علينا أن نشمله كجزء من نهجنا".

يجب أن تكون إتاحة مجال أوسع للقراصنة وغيرهم من خبراء الحاسب المستقلين أولوية خلال السنوات القادمة. ونحن نتوقع من الحكومات الغربية الاستمرار في محاولتها دمجهم سواء أفعلت ذلك علناً؛ عبر برامج شبيهة بسي.أف.تي، أم سراً عبر قنوات وكالات الاستخبارات. وستضع الحكومات ثقلها للحصول على نظراء افتراضيين في البلدان الأجنبية لاستكمال عامليها وأصولها السرية في العالم الفيزيائي. وستجنّد القراصنة وغيرهم من الأفراد الضليعين تقنياً لكي يكونوا مصادر تتعامل معهم عن بعد عبر قنوات آمنة على الشبكة. لكن، ثمة تحديات غير مباشرة تنطوي عليها الأصول الافتراضية. فعلى الرغم من فائدتها، ستغيب عنها التفاعلات الشخصية التي لطالما اعتمد عليها عاملو الاستخبارات على مدى عقود لتحديد مصداقية مصادرهم. من الصعب القول إن محادثة الفيديو تقدم بديلاً، لذا سيترتب على الوكالات أن تجد طريقة فعالة للتدقيق في المشاركين الجدد. وقد تكون الثقة بالأصول الافتراضية أصعب من عملية تجنيدها في الواقع.

عقب أخيل عند الإرهابيين

سيجد الإرهابيون في المستقبل أن التقانة ضرورية لكنها محفوقة بالمخاطر. وقد كان موت أسامة بن لادن عام 2011 نهايةً فعلية لحقبة الإرهابيين المقيمين في الكهوف والمعزولين عن البيئات التقانية الحديثة. إذ كان بن لادن قد تخفى طوال خمس سنواتٍ على الأقل في منـزله في أبوتا باد في باكستان من دون إنترنت أو

هواتف نقالة. حيث كان عليه الابتعاد عن الشبكة لكي يبقى في مأمن؛ الأمر الذي حصر مجاله ونفوذه إلى درجة كبيرة في شبكة القاعدة التي كانت تعتمد - جزئياً على الأقل - على الاتصالات في عملها. ومن سخرية القدر أن غياب اتصال الإنترنت في منـزل ريفي ضخم هو الذي ساعد على التعرف عليه بعد أن أشار مراسله لعاملي الاستخبارات إلى الاتجاه الصحيح.

مع أن بن لادن ربما تجنب الأسر ببقائه بعيداً عن الشبكة، إلاّ أنه اضطر إلى استخدام أقراص الفلاش والأقراص الصلبة والدي.في.دي لكي يبقى على اطلاع بما يحصل. وقد مكنته هذه الأدوات من تتبع عمليات القاعدة الدولية، ووفرت طريقةً فعالةً لمراسليه ينقلون من خلالها كميات كبيرة من البيانات بينه وبين الخلايا المختلفة في أماكن أخرى. وطالما كان طليقاً، ظلت هذه المعلومات على هذه الأجهزة آمنةً، ويستحيل الوصول إليها. لكن، عندما أغار فريق البحرية السادس على منـزله صادر أجهزته، لتكون غنيمته ليس الرجل الأكثر ملاحقةً في العالم فقط، بل ومعلوماتٍ خطيرة عن كل شخصٍ كان يتعامل معه.

لكن السيناريو الأكثر قابلية للاستمرار خلال العصر الرقمي الجديد سيكون شبيهاً بهجمات بومبـي عام 2008 حين قام عشرة رجالٍ ملثمين بأخذ المدينة رهينةً في حصارٍ لمدة ثلاثة أيام قتل خلالها 174 شخصاً، وجرح أكثر من ثلاثمئة. حيث اعتمد المسلحون على تقانات المستهلك البسيطة (أجهزة بلاك بيري وغوغل إيرث والاتصالات الصوتية على الإنترنت) لتنسيق الهجمات وتوجيهها. فكانوا يتواصلون مع مركز قيادة في باكستان، حيث كان قادتهم يشاهدون تغطيةً حية للأحداث على تلفازٍ فضائي، ويتابعون الأخبار لتقديم توجيهاتٍ تكتيكية بالزمن الحقيقي. لقد جعلت التقانة هذه الهجمات أكثر فتكاً بكثير مما كان لها أن تكون من دونها. لكن، ما إن ألقي القبض على آخر مسلحٍ (والناجي الوحيد) حتى تمكن المحققون، باستخدام المعلومات التي قدمها هو إضافةً إلى المعلومات الأكثر خطورة التي تُركت على أجهزة رفاقه، من اقتفاء آثارٍ إلكترونية أوصلتهم إلى أشخاص وأماكن هامة في باكستان ما كان من الممكن الوصول إليها قبل أشهر، إن أمكن ذلك أصلاً.

لكن ما يدعو إلى التفاؤل إزاء الإرهاب السايبري هو أن ممارسيه لن يتاح لهم - على جميع الجهات تقريباً - مجال لارتكاب خطأ كبير. فمعظمنا ليس لديه ما يدفعه للتفكير بالتغير الذي سيطرأ على تفاعله مع التقانة حين تكون حريته أو حياته معتمدة على حذف الآثار التي يتركها عندما يستخدم الإنترنت. فالإرهابيون السايبريون يتمتعون بمعارف تقانية عالية على نحو استثنائي، لكن ماذا عن أصدقائهم؟ وماذا عن أقاربهم الذين يتفاعلون معهم؟ إن توقع سلوكٍ منضبط تماماً من كل إرهابـي على الإنترنت غير واقعي. ولنأخذ مثالاً من غير الإرهابيين هو جون ماكافي، المليونير ورائد برمجيات مكافحة الفيروسات الذي أصبح هارباً دولياً بعد أن فرّ من السلطات التي أرادت استجوابه بشأن جريمة قتل راح ضحيتها جاره في وطنه الاختياري بليز. فبعد دعوته صحفيين من مجلة فايس التي تصدر على الإنترنت لإجراء مقابلةٍ معه في مخبئه السري، وقف ماكافي لالتقاط صورةٍ له مع رئيس تحرير المجلة، وتم التقاط الصورة بجهاز أي فون 4.أس. لكن ما لم يكن

يعلمه هو (ولا من أجرى المقابلة معه) هو أن نشر صورته سيشي بموقعه أيضاَ، لأن الكثير من الهواتف الذكية (ومنها هاتف أي فون 4.أس) تُضمِّن بياناتٍ فوقية في الصور التي تلتقط بكاميراتها تحتوي على إحداثيات جي.بـي.أس. ولم يتطلب الأمر سوى أن يلاحظ أحد مستخدمي تويتر البيانات الفائقة لتعلم السلطات، والعالم بأسره، فجأةً أن ماكافي في غواتيمالا قرب بركة سباحةٍ في مطعم رانشون ماري. لقد كان على مجلة فايس أن تعلم (فنحن نعرف عن بيانات الموقع الفائقة منذ سنوات)، لكن مع ازدياد تعقيد الهواتف الذكية المستمر، يزداد قدر التفاصيل الصغيرة التي تجب متابعتها.

مع انتقال الحياة الاجتماعية والمهنية والشخصية إلى الفضاء السايبري أكثر فأكثر، سيزداد التواصل البيني القائم بين جميع الفعاليات الرقمية بشكل هائل. والحواسب تجيد التعرف على النماذج وحل مشكلات .

وبتوفر المزيد من البيانات، يمكن للخوارزميات الحاسوبية أن تحسب مدى الارتباطات الإحصائية وتصل إلى توقعات أكثر دقة، وبسرعةٍ أكبر ممّا يستطيع أي إنسان القيام به. فتخيل متطرفاً مغربياً في فرنسا قام بكل شيءٍ ممكن لكي يبقي هوية هاتفه الذكي المتصل بالشبكة النقالة مغفلة؛ فعطل معلومات الموقع الجغرافي، وخرج من جميع خدمات مشاركة البيانات، وواظب على إزالة بطاقة السيم الخاصة به بشكلٍ دوري تحسباً لتقفي أثرها من قبل أي شخص، كما عوَّد نفسه أيضاً على إخراج البطارية من الهاتف كإجراءٍ احترازي أخير، لأنه يعلم أنه حين يتم إطفاء الهاتف تبقى البطارية محتفظةً بالطاقة اللازمة لإرسال الإشارات واستقبالها. ورقم هاتفه رقم بسيط من بين الآلاف من الأرقام، ويستحيل أن يلفت الأنظار أو أن يتم ربطه بصاحبه أو بموقعه. إلا أن السلطات تعلم أنه مولعٌ بالمراهنة في سباقات الخيل، وهي تعلم أيضاً بوجود أربعة مواقع رهان خارج الحلبة في بلدته. لذا يمكنها، باستخدام هذه البيانات، تضييق مجموعة الأرقام المحتملة من عدة آلاف إلى بضع مئات أو ما شابه من الأرقام التي تتردد على هذه الأماكن. ولنقل أيضاً إن بعضاً من معارفه لا يُبدون القدر نفسه من الحذر الذي يبديه هو إزاء بياناتهم. عندها، يمكن للسلطات أن تربط بين مجموعة الأرقام التي تتردد على أماكن الرهان مع مواقع أصدقائه المختلفة، وربما يكون هذا كل ما تحتاج إليه لتحديد رقمه. كان تخيل مثل هذا النوع من التحقيقات المشتملة على بيانات كبيرة غير ممكن ذات يوم، لكنه أصبح سهلاً اليوم كمثال جديد على تقاسم البشر والحواسب الواجبات. فسواء أكنا على الشبكة أم خارجها، تقدم نشاطاتنا (ونشاطات أصدقائنا وعائلاتنا وديموغرافيتنا) لأنظمة الحواسب الذكية معلوماتٍ أكثر من كافية لتحديد هويتنا.

سيكون خطأ واحد أو ارتباط ضعيف واحد كفيلاً بالإيقاع بشبكة كاملة. وقد شرح لنا أحد أعضاء فريق البحرية الأمريكي السادس - سبق أن تحدثنا معه - عن أحد القادة الكبار في القاعدة. فقد كان حذراً على نحو استثنائي في ما يتعلق بالتقانة، وكان يبدل هواتفه باستمرار، وقلما كان يتحدث لوقتٍ طويل. لكن، مقابل الحرص الذي كان يبديه في حياته المهنية، كان مهملاً في حياته الاجتماعية. فقد اتصل ذات مرة بقريبٍ له في أفغانستان، وذكر له أنه ينوي حضور حفل زواج، فأدت هذه

الخطوة الخاطئة إلى تسريب ما يكفي من المعلومات للسلطات؛ ممّا أدّى إلى العثور عليه وإلقاء القبض عليه. فما لم يكن الإرهابـي وحيداً تماماً في نشاطاته (وهذا أمرٌ نادر) ومنضبطاً انضباطاً تاماً على الإنترنت (وهذا أكثر ندرة بعد)، سيبقى هناك احتمال كبير جداً بأن يوقع بنفسه بطريقة ما في محطة ما من سلسلة الأحداث التي تقود إلى الهجوم المخطط له. فكثيرة جداً هي الطرق التي يكشف بها المرء عن نفسه أو يتم الكشف بها عنه؛ وهذا أمرٌ مشجع عند التأمل في مستقبل مكافحة الإرهاب.

إلى جانب الإرهابيين السايبريين الأذكياء والعارفين، سيكون هناك بالطبع إرهابيون أغبياء أيضاً. وفي فترة التجربة والخطأ التي ترافق نمو الاتصالات، سيظهر نقص الخبرة بطرق كثيرة قد تبدو مضحكةً بالنسبة إلى أولئك الذين نشأوا مع الإنترنت منا. فبعد ثلاث سنواتٍ على خطف الصحفية الكندية أماندا ليندهاوت في الصومال (حيث أخذت رهينةً لخمسة عشر شهراً من قبل متطرفين شباب وأطلق سراحها أخيراً مقابل فديةٍ كبيرة). اتصل بها خاطفوها السابقون عبر الفيسبوك وقاموا بتهديدها، وطالبوها بمزيدٍ من المال. وكانت بعض الحسابات التي استخدموها حساباتٍ شكلية تم إنشاؤها لهدفٍ وحيد هو مضايقة والدها. لكن حساباتٍ أخرى بدت أصلية، ولم يبد أن الإرهابيين يدركون الدرجة التي يكشفون بها عن أنفسهم بهذه الطريقة. إذ لم تشتمل هذه الحسابات على أسمائهم وحساباتهم فقط، بل وعلى كل من يرتبطون به، وكل شيء قاموا بكتابته على صفحاتهم الخاصة أو على صفحات الآخرين على الفيسبوك، ومواقع الإنترنت التي تعجبهم وهلم جرًّا. وكل شيءٍ ينكشف بهذه الطريقة سيكون بمثابة درس للمتطرفين الآخرين يمكّنهم من تجنب الأخطاء المشابهة في المستقبل.

تقدر نسبة الناس الذين يقتنون هواتف نقالة، والذين يبقون هواتفهم ضمن مسافة ثلاث خطواتٍ منهم لمدة أربع وعشرين ساعة في اليوم بأكثر من 90 بالمئة. وما من سبب للاعتقاد بأن ذلك لن ينطبق على المتطرفين، فقد يعتمدون إجراءات جديدة تساعد في حمايتهم (مثل إزالة البطاريات من هواتفهم بشكلٍ دوري)، لكنهم لن يكفوا عن استخدامها تماماً؛ مما يعني أن مداهمات مكافحة الإرهاب التي يقوم بها الجيش والسلطة التنفيذية ستأتي بنتائج أفضل؛ إذ ستؤدي إلى إلقاء القبض على الإرهابـي وعلى أفراد شبكته. وستبقى تحقيقات ما بعد الاعتقال هامةً أيضاً، لكن كل الأجهزة التي استخدمها الإرهابـي (من هواتف نقالة، وسواقات تخزين، وحواسب محمولة، وكاميرات) ستكون منجم ذهبٍ محتملاً. إذ يمكن عبر الاستيلاء على أجهزة الإرهابـي المأسور - من دون علم شبكته - أن يكشف رفاقه من دون أن يقصدوا عن معلوماتٍ ومواقع حساسة. كما أن الأجهزة قد تحمل محتويات يمكن استخدامها لكشف الرياء الذي يلف الشخصية العامة للإرهابـي؛ كما فعل المسؤولون الأمريكيون عندما كشفوا عن احتواء الحاسب الذي أخذ من أسامة بن لادن على مخزونٍ سري هائل من ملفات الفيديو الإباحية. ولا شك في أن الإرهابيين الأكثر حنكةً، حين تنكشف لهم نقاط ضعفٍ كهذه، سيسعون إلى معالجتها بسيلٍ من المعلومات المضللة. وسيكون تخزين تفاصيل شخصية تعود لمنافسين أو أعداء

عمداً على الأجهزة التي يعلمون أنها ستقع في أيدي السلطات التنفيذية شكلاً مفيداً من أشكال التخريب.

ممنوع تخفي الأشخاص

مع تطوير الإرهابيين طرائق جديدة سيتم تكييف استراتيجيات مكافحة الإرهاب وفقاً لها. لذلك ربما يكون السجن غير كافٍ لاحتواء شبكةٍ إرهابية، وقد ترتئي الحكومات على سبيل المثال أن وجود مواطنين مفصولين عن النظام البيئي التقاني ينطوي على مخاطر كبرى. ولا شك في أن هناك دائماً أشخاصاً في المستقبل - كما اليوم - يعارضون تبني التقانة واستخدامها، وأشخاصاً لا يريدون أن يربطهم أي شيء بالحسابات الافتراضية ونظم البيانات الشبكية أو الهواتف الذكية. إلا أن الحكومات قد يساورها الشك في أن أولئك الذين ينأون بأنفسهم كلياً ربما يكون لديهم شيء ما يخفونه، وهم بالتالي أكثر ميلاً إلى خرق القوانين. وستقوم الحكومة كإجراءٍ لمكافحة الإرهاب ببناء نوعٍ من سجل الذي سبقت الإشارة إليه سابقاً. فإذا لم تكن لديك حسابات على الشبكات الاجتماعية أو اشتراك هاتفٍ نقال، وثمة صعوبة غير اعتيادية في إيجاد أية إشارة لك على الإنترنت، فربما تعتبر مرشحاً لدخول مثل هذا السجل. بل ربما يتم إخضاعك لمجموعة قاسية من الضوابط الجديدة؛ كالكشف الصارم في المطار، أو حتى لقيود على السفر.

ترتئي الحكومات وليس تقرر

يمكننا في عالم ما بعد الحادي عشر من أيلول أن نتلمّس منذ اليوم مؤشراتٍ تدل على أن كل البلدان، حتى تلك التي تتمتع بأسسٍ قوية للحريات المدنية ستتخلى عن حصانات مواطنيها من أجل نظامٍ يؤمن للوطن مزيداً من السيطرة والأمن، وهو توجهٌ لن يزداد إلا تسارعاً. فبعد أن يحقق الإرهابيون السايبريون بعض النجاحات، سيسهل إقناع الناس بأن التضحيات المطلوبة منهم (رفع مستوى مراقبة الحكومة للنشاطات على الشبكة قبل كل شيء) تستحق العناء لما ستعود به عليهم من راحة بال. لكن الضرر الذي سيرافق هذا السيناريو - إذا وضعنا جانباً ملاحقة عددٍ ضئيل من البسطاء الأبرياء - يتمثل بالطبع في خطر استغلال عاملي الحكومة له أحياناً أو إساءتهم للحكم. وهذا سبب جديد يضاف إلى الأسباب المعروفة للنضال من أجل الخصوصية والأمن في المستقبل.

ستزداد أهمية عملية الجذب والدفع هذه بين الخصوصية والأمن خلال العصر الرقمي في السنوات القادمة. وستحتاج السلطات المسؤولة عن تحديد الأفراد الخطرين ومراقبتهم وإلقاء القبض عليهم إلى نظم إدارة بيانات ضخمة ومتطورة جداً لتنفيذ مهامها. وبالرغم ممّا يقوم به الأفراد والمنظمات والمجموعات غير الربحية الملتزمة لحماية الخصوصية، لا مفر من احتواء هذه النظم على مقادير هائلة من البيانات حول المواطنين غير الإرهابيين (ويبقى السؤال القائم هو مقدار هذه البيانات ومكانها). فمعظم المعلومات التي تقوم الحكومات بجمعها عن شعبها اليوم (كالعناوين وأرقام الهويات، والسجلات الجنائية، وبيانات الهواتف النقالة)

تخزن في أماكن معزولة (أو لم تتم رقمنتها بعد في بعض البلدان). وعزل هذه الأماكن يضمن درجة من الخصوصية للمواطنين، لكنه يعطل إلى حدٍّ كبير فعالية المحققين.

وهنا يكمن تحدي الذي تواجهه الهيئات الحكومية وغيرها من المؤسسات في أنحاء العالم. فكيف يمكن لوكالات الاستخبارات، والأقسام العسكرية، والسلطات التنفيذية دمج جميع قواعد بياناتها الرقمية في بنيةٍ مركزية تسمح بالربط بين النقاط الصحيحة من دون انتهاك حقوق الخصوصية للمواطنين؟ ففي الولايات المتحدة على سبيل المثال، يستخدم مكتب التحقيقات الفيدرالي ووزارة الخارجية والسي.آي.أيه وغيرها من الوكالات الحكومية أنظمة مختلفة. ونحن نعلم أن الحواسب قادرة على إيجاد النماذج المتكررة والحالات الشاذة وغيرها من المؤشرات ذات المعنى بفعالية أكبر بكثير من قدرات المحلل البشري، إلا أن ضم أنظمة معلومات متباينة (كمعلومات جوازات السفر، ومسوحات البصمات، والكشوفات البنكية، وسجلات التنصت على المكالمات، وبيانات السفر) وبناء خوارزميات تقاطع بينها على نحو فعال، فتزيل التكرارات وتتعرف على مكامن الخطر في البيانات، مهمة في غاية الصعوبة، وتحتاج إلى وقتٍ طويل لإنجازها.

لكن الصعب ليس مستحيلاً، وجميع المؤشرات تدل على أن نظم المعلومات المدمجة الشاملة هذه تتحول تدريجياً إلى معيار ستتبناه الدول الحديثة الموسرة في المستقبل القريب. وقد أتيحت لنا فرصة إجراء جولةٍ في مركز قيادة بلاتفورما في المكسيك، الذي يحتوي على قاعدة بيانات جنائية وطنية تثير الإعجاب، وربما كانت أفضل نموذج لنظام بيانات مدمج قيد التشغيل اليوم. إذ تجمع قاعدة البيانات الضخمة هذه، والمقامة في ملجأ تحت الأرض في أمانة سر مجمع الأمن العام في مدينة مكسيكو، بين المعلومات الاستخباراتية والتقارير الجنائية وبيانات الزمن الحقيقي المجموعة من كاميرات المراقبة ومدخلات أخرى من وكالات وولايات في جميع أنحاء البلاد. وتقوم خوارزميات خاصة باستخراج النماذج المتكررة، وتعرض رسوماً بيانية اجتماعية، وتراقب المناطق المضطربة بحثاً عن مؤشرات العنف والجريمة. كما تساعد أيضاً على مراقبة الكوارث الطبيعية وغيرها من الحالات الطارئة في المدنية. إن مستوى المراقبة والتقدم التقاني الذي تتمتع به بلاتفورما في المكسيك والذي اطلعنا عليه يعتبر خارقاً، لكن التحديات الأمنية التي ستواجهها السلطات المكسيكية ستكون كذلك أيضاً.

في مستهل هذا القرن، وبعد الهجمات الإرهابية التي وقعت في الحادي عشر من أيلول، طرح شيء مشابه في الولايات المتحدة، حيث أعدّت وزارة الدفاع وأعطت الضوء الأخضر لتطوير برنامجٍ يدعى الاطلاع المعلوماتي الشامل (تي. آي. إي). وتم تصميم البرنامج - الذي اعتبر أقصى ما يمكن لجهاز أمني أن يصل إليه في اكتشاف النشاطات الإرهابية - وتمويله؛ حيث يجمع جميع بيانات (بما فيها السجلات المصرفية ومشتريات البطاقات الائتمانية والسجلات الطبية)، إضافة إلى الأجزاء الأخرى من المعلومات الشخصية،

لإنتاج فهرس مركزي قابل للبحث تستخدمه السلطات التنفيذية ووكالات مكافحة الإرهاب. وثمة تقانات متقدمة لتنقيب البيانات سيتم تطويرها لاكتشاف النماذج المتكررة والارتباطات؛ حيث تتكفل التي يتركها الأشخاص الخطرون خلفهم بالكشف عنهم في الوقت المناسب منعاً لوقوع هجوم جديد.

عندما خرجت تفاصيل البرنامج إلى العلن، تعالت موجة من الانتقادات، من اليمين واليسار في آنٍ معاً، محذّرة من التبعات المحتملة للبرنامج على الحريات المدنية والخصوصية والأمن على المدى الطويل. وركزت هذه الأصوات على احتمالات استغلال النظام لهذا القدر الهائل من المعلومات، ووصفت البرنامج بأنه

في أهدافه، وفي النهاية نجحت حملةٌ في الكونغرس لإغلاق البرنامج في اتخاذ تدابير كفيلة بحجب أي تمويل قد يوجه للبرنامج عبر مجلس الشيوخ في لائحة مخصصات الدفاع لعام 2004، وتم إغلاق مكتب الاطلاع المعلوماتي نهائياً؛ وإن كانت بعض مشاريعه قد وجدت ملجأً لها في ما بعد لدى وكالات استخباراتية أخرى في القطاع الأمني الحكومي المتناثر عبر البلاد.

سيكون الصراع من أجل الخصوصية طويلاً وفي غاية الأهمية. وإذا كنا قد كسبنا بعض المعارك الأولى فإن الحرب أبعد ما تكون عن نهايتها. فالمنطق الأمني لن يكفّ بشكلٍ عام عن إثارة المخاوف المتعلقة بالخصوصية. وليس على صقور السياسة سوى الانتظار حتى يطرأ حدث عام على جانب من الخطورة لكي يجدوا الإرادة والدعم السياسيين اللازمين للدفع بمطالبهم قدماً، وليملوا إرادتهم فوق الاعتبارات التي تعبر عنها الحمائم فيصبح فقدان الخصوصية بعدها أمراً اعتيادياً. مع منصات معلوماتٍ موحدة كهذه، لا بد من اتخاذ سبل الوقاية المناسبة لحماية المواطنين والحريات المدنية بحزم منذ البداية، لأنه سيكون من السهل جداً تجاوزها بمجرد ظهور تهديدٍ أمني جدي (فالمعلومات موجودة مسبقاً لمن يريد أخذها). ولا بد أن الحكومات التي تشغل منصات المراقبة ستنتهك القيود المفروضة عليها (عبر التشريع أو الحكم الشرعي) في النهاية، لكن من الممكن في الدول الديموقراطية التي تتمتع بنظم قانونية فاعلة كما يجب وبمجتمعات مدنية نشيطة تصحيح مثل هذه الأخطاء، سواء أفعلت ذلك عبر معاقبة المذنبين أم بوضع إجراءاتٍ وقائيةٍ جديدة.

تبقى أمام الدول المسؤولة أسئلةٌ صعبة. فإمكانية إساءة استخدام هذه السلطة مرتفعةٌ إلى حد مرعب، ناهيك عن الأخطار الناجمة عن الخطأ البشري والفضول والحالات الإيجابية الزائفة الناتجة عن البيانات. فنظام معلومات موحد بشكل كامل كهذا، يجمع بين جميع أشكال مدخلات البيانات إضافة إلى برمجيات قادرة على تفسير السلوكيات وتوقعها، ويقوم البشر بتشغيله، ربما يمنح ببساطة قدراً من السلطة أكبر بكثير من أن يتمكن أي شخص من التعامل معه بمسؤولية. علاوةً على ذلك، ما إن يُبنى مثل هذا النظام، حتى يستحيل تفكيكه في ما بعد. وحتى إذا كانت حالةٌ أمنية خطيرة على وشك التطور، فأيّ حكومة ستتخلى طوعاً عن أداةٍ تنفيذية بهذه القوة؟ أما الحكومة التي ستستلم زمام السلطة بعد ذلك، فإنها لن تبدي المقدار نفسه من الحذر والمسؤولية إزاء المعلومات التي لديها كما فعلت الحكومة السابقة. وهذه الأنظمة الموحدة للمعلومات لا تزال في طور الطفولة الآن، ولا

شك في أن تحدياتٍ مختلفة (مثل الجمع المنتظم للبيانات) ستكبحها عبر فرض قيود على فعاليتها. لكن هذه المنصات ستتحسن، وثمة هالة من الحتمية تحيط بإمكانية انتشارها في المستقبل، والعلاج الوحيد للطغيان الرقمي المحتمل هو تقوية المؤسسات القانونية، وتشجيع المجتمع المدني ليبقى فعالاً ومدركاً لاحتمالات إساءة استخدام هذه السلطة.

بمناسبة مناقشتنا لاستخداماته المستقبلية، ثمة بعد ملاحظة نهائية حول المحتوى الرقمي. فمع انتشار البيانات على الإنترنت، وتمكن أي شخصٍ تقريباً من إنتاج مقادير غير محدودة من المحتويات الفريدة وتحميلها وبثّها، سيكون التحدي الحقيقي متمثلاً في عملية التحقق من هذا المحتوى. فخلال السنوات القليلة الأخيرة تحولت محطات الأخبار الكبرى من استخدام مشاهد الفيديو الاحترافية فقط إلى قبول محتويات ينتجها مستخدمون، كأفلام الفيديو المنشورة على موقع يوتيوب. وعادةً، تشير هذه المحطات إلى عدم إمكانية التحقق من الفيديو بشكل مستقل، لكن عملية بثه تمثل في جوهرها تصديقاً ضمنياً لمحتواه. وقد ترتفع الأصوات المعارضة التي تقول إن الفيديو قد تعرض للتلاعب، أو إنه مضللٌ بطريقةٍ ما. لكن هذه المزاعم، إذا تم تسجيلها، لن تحظى سوى بقدرٍ قليلٍ من الاهتمام، وغالباً ما سيتم تجاهلها. وسيؤدي هذا التوجه لاستخدام محتويات لم يتم التحقق منها في النهاية إلى الدفع باتجاه تطبيق إجراءات تحقق أكثر صرامةً تكون مضبوطة تقنياً.

ستكتسب إجراءات التحقق بالفعل أهميةً أكبر في جميع جوانب حياتنا. وقد رأينا سابقاً كيف أن الحاجة إلى التحقق ستحدد شكل التجربة التي نعيشها على الشبكة، حيث ستفرض حمايات أفضل ضد انتحال الشخصية، كما ستغير البيانات البيومترية المشهد الأمني، وسيلعب التحقق دوراً هاماً أيضاً في تحديد التهديدات الإرهابية الصحيحة. وسيلجأ معظم المتطرفين إلى استخدام بطاقات سيم مختلفة وتغيير هوياتهم الشبكية، وإلى طيفٍ واسع من أدوات التشويش لتغطية آثارهم تجنباً للتعرف عليهم. وسيكون التحدي الذي ستواجهه السلطات التنفيذية هو إيجاد الطرق التي تمكنها من التعامل مع هذا التشويش في المعلومات من دون إضاعة ساعات العمل على الإنذارات الكاذبة. ومن شأن توفر سجلات المتخفين التخفيف من هذه المشكلة بالنسبة إلى السلطات لكنه لن يحلّها.

بما أن عموم الجماهير سيفضّلون بشكل عام الهويات المصدّقة على الإنترنت، وسيثقون بها ويعتمدون عليها ويصرّون عليها، فسيحرص الإرهابيون على استخدام قنوات التحقق الخاصة بهم عندما يطرحون ادعاءاتهم. وستتوفر طرق كثيرة للتحقق من مقاطع الفيديو والصور والمكالمات الهاتفية التي تستخدمها المجموعات الإرهابية في تواصلها. وسيصبح التقاط الصور مع الرهائن مع إظهار إصدار جديد من جريدة يومية عادة بالية، فالصورة بحد ذاتها ستظهر توقيت التقاطها ومحتواها؛ حيث ستسمح التقنيات الجنائية الرقمية، كالتحقق من العلامة المائية، لخبراء تقانة المعلومات بالتحقق ليس فقط من توقيت التقاط الصورة، بل ومن مكان التقاطها وطريقة التقاطها أيضاً.

إلا أن هذا الإصرار على التحقق من المحتويات سيتطلب من الإرهابيين الالتزام بتهديداتهم. فالإرهابـي الذي لا يلتزم يغامر بفقدان مصداقيته على نحو يسيء إلى سمعته وسمعة مجموعته. فإذا أصدرت القاعدة تسجيلاً صوتياً يثبت أن أحد قادتها قد نجا من غارة شنتها طائرة بلا طيار ووجد خبراء الحاسب الجنائيون باستخدام برمجيات تعرف على الصوت أن الصوت المسجل يعود لشخص آخر، فسيؤدي ذلك إلى إضعاف موقع القاعدة وتشجيع منتقديها. وكل تحدّ تفرضه إجراءات التحقق سيقلل من هيبة الكثير من المجموعات المتطرفة التي تعتمد على هيبتها لجمع التمويل، وللتجنيد، ولزرع الرعب في قلوب المجموعات الأخرى. وبذلك قد يصبح التحقق أداة جبارة في الحرب ضد التطرف العنيف.

معركة القلوب والعقول تنتقل إلى الشبكة

صحيح أن القراصنة وخبراء الحاسب المؤهلين سيزيدون من قدرات المجموعات الإرهابية، لكن القاعدة العريضة لعمليات التجنيد ستكون - كما هي اليوم - بين الجنود العاديين. وهؤلاء سيكونون من الشباب غير المتعلمين، وستكون لديهم مظالم يستغلها المتطرفون لمصلحتهم. ونحن نميل إلى الاعتقاد بأن التغيير الأهم في استراتيجية مكافحة الإرهاب في المستقبل لن يحدث في مجال المداهمة ومراقبة الهواتف الخلوية، بل سيركز بدلاً من ذلك على إزالة نقاط الضعف التي تعاني منها هذه الشرائح الاجتماعية التي تعيش تحت الخطر عبر إشراكها تقانياً.

تقدر نسبة البشر الذين لا تتجاوز أعمارهم الثلاثين عاماً بنحو 52 بالمئة في العالم. والغالبية العظمى منهم ينتمون إلى من نعتبرهم -
؛ إذ يعيشون في أحياء فقيرة في المدن، أو في تجمعات مهاجرين سيئة الاندماج، وفي أماكن يضعف فيها حكم القانون وتعاني من محدودية الفرص الاقتصادية. والفقر والإقصاء والإذلال ونقص الفرص وصعوبة التنقل، بل ومجرد الشعور بالملل، كلها أسباب تجعل الفئات الشابة على استعداد عالٍ للتأثر بالآخرين. ووجود مظالم مع خلفية من القمع في ثقافة ثانوية تحض على التطرف يغذي تحولهم إلى التطرف. وينطبق ذلك على طفل غير متعلم في حي فقير مثلما ينطبق على طلاب الجامعة الذين لا يرون أية فرص تنتظرهم على الضفة الأخرى بعد التخرج.

قمنا في غوغل آيدياز بدراسة التحول إلى التطرف في أنحاء العالم، وركزنا نظرنا بشكل خاص على الدور الذي يمكن أن تلعبه تقانات الاتصالات. فثبت لنا أن عملية تحول الإرهابيين إلى التطرف لا تختلف كثيراً عما نراه لدى عصابات المدن أو المجموعات العنفية كالعنصريين البيض. وفي مؤتمر الذي نظمناه في حزيران من عام 2011، جمعنا أكثر من ثمانين متطرفاً سابقاً لمناقشة أسباب انضمام الأفراد إلى المنظمات العنفية وأسباب تركهم لها. وعبر حوار مفتوح مع المشاركين، الذين كان في صفوفهم متطرفون دينيون وقوميون عنيفون وأفراد عصابات مدن وفاشيون من أقصى اليمين وأعضاء في منظمات جهادية، توصلنا إلى وجود دوافع مشتركة تجمع بين هذه المجموعات كلّها، وأن الدور الذي يلعبه

الدين والإيديولوجيا أضعف مما يعتقده معظم الناس. فأسباب انضمام الناس إلى المجموعات المتطرفة معقدة، وغالباً ما تكون مرتبطة بغياب شبكة دعم، وبالرغبة في الانتماء إلى مجموعة أو تمرد، أو البحث عن حماية، أو السعي وراء الأخطار والمغامرات.

ثمة الكثير جداً من الأشخاص الذين يتقاسمون هذه المشاعر. لكن الجديد هو أن الكثيرين منهم سيبثون همومهم على الإنترنت بطرق تروج لهم - سواء أتعمدوا ذلك أم لا - بين مجنِّدي الإرهابيين. وما يسعى إليه الشباب المتحوّلون إلى التطرف عبر ارتباطاتهم الافتراضية ينبع من تجربتهم في العالم المادي، أي مما عانوه من خذلان ورفض وعزلة ووحدة وإساءة معاملة. ويمكننا استكشاف الكثير عنهم في العالم الافتراضي، لكن نـزع فتيل التطرف حقاً سيتطلب في النهاية لقاءات جماعية، والكثير من الدعم والمعالجة، وبدائل هادفة في العالم المادي.

تقوم غوغل، مثل شركات كثيرة غيرها، ببناء أدوات مجانية يمكن لأي شخص استخدامها. لذا، إنّ الشركة تعمل باستمرار على فهم كيف يمكن التخفيف من احتمال أن يستخدم أفراد أو كيانات عدوانية هذه الأدوات لإلحاق الأذى بالآخرين.

لن تكون الكلمات والخطابات التي تلقى ضد التطرف العنيف كافيةً في المعركة من أجل كسب قلوب الشباب وعقولهم. كما لن تنفع القوة العسكرية، فقد حققت الحكومات نجاحاتٍ كبيرة في القبض على الإرهابيين الموجودين وقتلهم، لكنها كانت أقل فعالية في وقف تدفق المجندين. وكما روى الجنرال ستانلي ماكريستال القائد السابق لقوات الولايات المتحدة والناتو في أفغانستان لمجلة دير شبيغل عام 20 فإن "ما يهزم الإرهاب هو في الحقيقة شيئان، أولهما فرض القانون، وثانيهما منح الفرص للناس. أي إنه إذا كان لديك حكم يسمح لك بتطبيق القانون، فلديك بيئة تصعب فيها ممارسة الإرهاب. وإذا كانت لديك فرص تقدمها للناس في حياتهم، وتسمح لهم من خلالها بأن يتعلموا ويجدوا فرصة عمل، فإنك تزيل أكبر سبب من أسباب الإرهاب. فالطريق الحقيقية لهزيمة الإرهاب ليست الضربات العسكرية وإنما الاهتمام بالشرطين الأساسيين".

إن وجهة نظر ماكريستال تسلّط الضوء على فرصة مفتوحة أمام المتحمسين للتقانة والشركات على حدٍّ سواء. فهل من طريقة أفضل لتحسين جودة حياة الشعب من تعزيز الاتصالات لديه؟ إن المكاسب التي تعود بها تقانات الاتصالات على المجتمعات (من فرص اقتصادية، وترفيه، وحرية معلومات، وزيادة في الشفافية وإمكانيات المحاسبة) تساهم جميعها في إنجاز مهمة نـزع فتيل التطرف. وعندما يصبح قطاع واسع من الشعب متصلاً بالإنترنت تصبح تعبئة الأوساط الافتراضية المحلية أمراً ممكناً؛ حيث ترفض العنف وتطالب القادة بالمحاسبة والتصرف. وستكون الأصوات التي ترتفع في وجه التطرف أكثر من تلك التي ترتفع لصالحه. فبينما قد تزيد التقانة من المدى الذي يمكن للأصوليين أن يصلوا إليه، فإنه سيستحيل استخدام الوعظ كوسيلة للترويج لطريقة معينة في التفكير من دون أن يترافق مع طريقة أخرى. إن كل الأشياء التي ترافق وجود وسط افتراضي فعال (من توفر المزيد من المناقشات والمزيد من وجهات النظر والمزيد من الخطابات

المتعاكسة) من شأنها أن تدخل الشك إلى قلوب هذه الفئات الشابة المطواعة، وأن تروج لاستقلالية التفكير بينهم. وبالطبع، إن كل ما سبق سيجد آذاناً صاغية إذا أدت الاتصالات إلى إنتاج فرص العمل.

ستكون استراتيجية نـزع فتيل التطرف الأكثر نجاعة هي تلك التي تركّز على الفضاء الافتراضي الجديد، حيث توفر للشباب بدائل غنية بالمحتويات، وتسالي تجعل اللجوء إلى الإرهاب آخر ملاذ قد يلجأون إليه. ويجب أن تُتخذ هذه التدابير على نطاق واسع، وأن يشترك فيها مساهمون من جميع الخلفيات؛ من القطاع العام إلى الشركات الخاصة، مع بناء الشراكات بين الفاعلين المحليين والناشطين في الخارج. وستلعب التقانة النقالة تحديداً الدور الأهم في هذه الحملة بما أن غالبية من يدخلون الإنترنت سيستخدمون أجهزتهم النقالة للقيام بذلك. وتمثل الهواتف منصات شخصية قوية، وهي رمز للمكانة، ويعتمد عليها مستخدموها ويثمنونها عالياً. والوصول إلى الشبان الساخطين عبر هواتفهم النقالة أفضل هدف يمكننا أن نسعى إليه.

لن تكون الحكومات والشركات الغربية هي التي تطوّر القسم الأعظم من المحتوى الجديد. فأفضل الحلول ستكون فائقة المحلية وسيصممها ويدعمها أشخاص ملمون بالبيئة القريبة إلماماً دقيقاً. وسيكون بناء منصاتٍ على أمل أن يحبها الشباب الن‍ـزقون ويستخدمونها أشبه بإلقاء قصاصات الدعاية من طائرة.

أما الغرباء فليس عليهم تطوير المحتوى، وإنما فقط إنتاج الفضاء. فإذا زودت المدينة بشبكة، وأعطيت الناس الأدوات الأساسية، فإنهم سينجزون جل العمل بأنفسهم. وقد طور عددٌ من شركات التقانة أدوات للمبتدئين تمكن الناس من بناء التطبيقات فوق منصاتها؛ ومجموعة خدمات وب أمازون ومحرك تطبيقات غوغل من بين الأمثلة على ذلك. إنّ إنتاج الفضاء الذي يسمح للآخرين ببناء أعمالهم وألعابهم ومنصاتهم ومنظماتهم مشروع تعاوني متبصر؛ لأنه يضمن أن يتم استخدام منتجات الشركة (مما يعزز الولاء لعلامتها أيضاً)، ويسمح للمستخدمين في الوقت نفسه ببناء ما يريدونه وبتشغيله بالفعل. أي سيقوم الصوماليون ببناء تطبيقاتٍ تُستخدم كأدواتٍ فعّالة لن‍ـزع فتيل التطرف، وللوصول إلى الصوماليين الآخرين. وهذا ما سيفعله الباكستانيون مع الباكستانيين الآخرين. وسيتاح أمام السكان المحليين المزيد من الفرص لبناء أعمالهم الصغيرة وإيجاد منافذ للشباب في الوقت نفسه. والمفتاح هنا ببساطة هو تمكين الناس من تكييف المنتجات بالطرق التي تتناسب مع حاجاتهم من دون أن تتطلب خبرة تقانية واسعة.

ستزيد هذه العملية من زخم الشراكات العامة - الخاصة مع الناشطين المحليين والأفراد ذوي النفوذ. وعلى الشركات أن تسعى أيضاً إلى إقامة الشراكات مع المجموعات المحلية لتطوير المحتويات. وفي الحالة المثالية، سينجم عن ذلك طيف من المحتويات والمنصات والتطبيقات يخاطب كل وسطٍ على حدة، ويحافظ في الوقت نفسه على المكونات التقانية والبنيوية المشتركة بما يمكّن من محاكاتها في أماكن أخرى. وإذا كانت قضايا التطرف متشابهةً في كل مكان، فإن أدويتها قد تكون كذلك أيضاً.

تتمتع شركات التقانة بموقع فريد يؤهلها لقيادة هذه المساعي على المستوى الدولي، وكثيرة هي الشركات البارزة التي تحمل جميع قيم المجتمع الديموقراطي من دون أن تثقل كاهلها الأعباء التي تفرض عليها الحكومة حملها. إذ يمكنها أن تذهب إلى حيث لا تستطيع الحكومة الذهاب، وأن تخاطب الناس بعيداً عن الرادارات الدبلوماسية، وأن تعمل باللغة الحيادية العالمية للتقانة. علاوةً على ذلك، هذه هي الصناعة التي تنتج ألعاب الفيديو والشبكات الاجتماعية والهواتف النقالة، وربما يكون لديها أفضل فهمٍ لكيفية جذب الشباب من أي قطاع. فالشباب تحديداً هم الفئة السكانية التي تستهدفها المجموعات الإرهابية بالتجنيد، فقد لا تفهم الشركات في أمور التطرف الدقيقة، أو في الفروقات الدقيقة بين مكوناتٍ ديموغرافية معينة في المسارح الرئيسة كاليمن والعراق والصومال، لكنها تفهم الشباب، وتعرف الألعاب التي تشدّ انتباههم. وفقط عندما نحوز اهتمام الشباب، نستطيع أن نأمل بالفوز بقلوبهم وعقولهم.

بالإضافة إلى ما سبق، نتيجة تورط شركات التقانة في التهديدات الأمنية (حيث تستخدم منتجاتها من قبل الإرهابيين)، سينتهي الأمر بالجمهور إلى مطالبتها بفعل المزيد ضد التطرف. ولا يعني ذلك تحسين منتجاتها وحماية المستخدمين عبر سياسات صارمة في ما يتعلق بالمحتويات والأمن فقط، بل أيضاً اتخاذ موقف علني. فتماماً كما أدى استسلام ماستر كارد وباي بال للضغوط السياسية في قصة ويكيليكس البطولية إلى إقناع الكثير من الناشطين بأن هاتين الشركتين قد اتخذتا موقفاً غير محايد، سيرى البعض في التزام شركات التقانة للصمت موقفاً غير مبرر. وسواء أكان ذلك عادلاً أم لا، فإن الشركات ستتحمل مسؤولية الاستخدامات المدمرة لمنتجاتها. وستكشف الشركات عن شخصياتها وقيمها الجوهرية وفقاً لطريقة نهوضها لمواجهة هذه التحديات، فالكلمات الفارغة لن ترضي جمهوراً مطلعاً.

يمكننا منذ اليوم ملاحظة خطوات مبكرة في هذا الاتجاه، مع إصدار بعض الشركات بيانات واضحة عبر سياساتها أو إجراءاتها، فموقع يوتيوب على سبيل المثال يواجه التحدي المتمثل بحجم المحتوى. فمع أربعة مليارات مقطع فيديو يتم استعراضها يومياً (وتحميل ستين ساعة فيديو كل دقيقة إلى الموقع)، سيستحيل على الشركة التدقيق في هذا المحتوى كله لمعرفة ما يمكن اعتباره مادةً غير ملائمة؛ كالمواد التي تدافع عن الإرهاب، لذا يعتمد يوتيوب بدلاً من ذلك على عملية يقوم المستخدمون خلالها بوضع إشارةٍ على المحتوى الذي يعتبرونه غير ملائم، ويحوّل الفيديو المعني إلى فريقٍ لدى يوتيوب لمراجعته، ويتم إغلاقه إذا كان يخرق سياسات الشركة. وسنشهد في النهاية ظهور معايير على مستوى الصناعة، حيث ستتبنى جميع المنصات الرقمية سياسةً موحدة في ما يتعلق بمقاطع الفيديو التطرفية الخطيرة المنشورة على الشبكة، كما توحدت على صياغة سياسات تحكم المشاهد الإباحية. والخط الذي يفصل الرقابة عن الأمن رفيع جدًّا، ممّا يفرض علينا اتخاذ التدابير الوقائية المناسبة. ستعمل الصناعة كرجلٍ واحد على تطوير برمجيات قادرة على تحديد مقاطع الفيديو ذات المحتوى الإرهابـي بطريقة أكثر فعالية. وقد

يصل الأمر بالبعض إلى استخدام برمجيات تعرف على الكلام تقوم بتسجيل سلاسل من الكلمات المفتاحية، أو برمجيات تعرف على الوجوه تقوم بالتعرف على الإرهابيين المعروفين.

لن يختفي الإرهاب بالطبع، بل سيستمر في تأثيره المدمر. لكن إرهابيي المستقبل مجبرون على العيش في العالمين المادي والافتراضي في آن معاً، وهو ما سيثقل على نموذج السرية والتكتم الذي يعتمدونه. وسيكون هناك قدر أكبر من العيون المراقبة والتفاعلات المسجلة، ولن يتمكن أحد - حتى أكثر الإرهابيين احترافاً - مهما بلغ به الحرص، من الاختفاء تماماً على الشبكة. فمتى تواجدوا عليها، صار من المكن العثور عليهم. وإذا أمكن العثور عليهم، فسيكون الوصول إلى كامل شبكاتهم وجميع مساعديهم أمراً ممكناً.

استكشفنا في هذا الفصل الطرق الأكثر غموضاً التي سيلجأ إليها الأفراد ليعطلوا عالمنا المستقبلي بعنفهم. لكن، إذا أخذنا بعين الاعتبار أن الحرب والنـزاعات جزء من التاريخ البشري بقدر ما هو المجتمع نفسه، فكيف ستنخرط الدول والحركات السياسية في هذه النشاطات لتحقيق آمالها؟ سنحاول اكتشاف الإجابة عن هذا السؤال بتخيل الآثار التي ستقع على النـزاعات والمعارك والتدخلات في عالم يكون الجميع فيه تقريباً على الإنترنت.

الفصل السادس: مستقبل النزاعات والمعارك والتدخلات

لم يسبق لنا الاطلاع على عدد كبير من الصراعات حول العالم كما يحصل حالياً، وتوفر المعلومات عن الفظاعات في مكان ما (من قصصٍ، ومقاطع فيديو، وصورٍ، وتغريدات) غالباً ما يجعل الأمر يبدو وكأننا نعيش في زمنٍ من العنف الاستثنائي. لكن، كما يقال في مجال الصحافة: "إذا سال الدم صعُد النجم"، فما تغير ليس عدد النـزاعات القائمة بل مدى بروزها اليوم.

إذا كان هناك ما يقال فهو إننا اليوم أكثر سلامة من أي وقت مضى؛ نظراً لتراجع مقدار العنف في المجتمعات البشرية تراجعاً سريعاً خلال القرون المنصرمة بفضل التطورات؛ مثل ظهور الدول القوية (التي تحتكر العنف وتنظم أو تُمأسس حكم القانون)، والتجارة (حيث يصبح الآخرون وهم أحياء أكثر قيمة من كونهم أمواتاً)، والشبكات الدولية الموسعة (التي تزيل الغموض عن الآخر وتجعله يبدو أكثر إنسانية). وكما يوضح العالم النفسي ستيفن بنكر في **الملائكة الأفضل لطبيعتنا** الذي يمثل مسحاً شاملاً وممتازاً لهذا التوجه، فإن القوى الخارجية التاريخية كالتعاطف والحس الأخلاقي والتعقل وضبط النفس التي "توجهنا بعيداً عن العنف وتحبب إلينا التعاون والإيثار". عندما ندرك هذا التحول، يلاحظ بنكر، "يبدأ العالم باتخاذ مظهر مختلف، فيبدو الماضي أقل براءة والحاضر أقل شرًّا".

لا شك في أن الاتصالات كانت ستدرج على لائحة بنكر لهذه القوى لو ألّف كتابه بعد ذلك بخمسين عاماً؛ لأن المستوى الجديد من الظهور الذي يواجه مرتكبـي العنف في عالمٍ مترابط - مع كل ما يبشر به - سيضعف إلى حدٍّ كبير ما يحفّز السلوك العنيف إضعافاً كبيراً، وسيغير حسابات الإرادة السياسية لارتكاب الجرائم ولإيقافها أيضاً.

إلا أن النـزاعات والحروب والصدامات الحدودية العنيفة والفظاعات الجسيمة ستبقى جزءاً من المجتمع البشري لأجيالٍ قادمة؛ حتى إذا غيرت شكلها بما يتلاءم مع العصر التقاني. سنستكشف في ما يلي العناصر المختلفة للنـزاعات (كاستشراء التمييز والاضطهاد والمعارك والتدخلات) وكيفية تغيرها خلال العقود القادمة استجابة لهذه المسؤوليات والعقوبات.

تراجع الإبادات وازدياد المضايقات

إن أصول النـزاعات العنيفة معقدة جداً حيث لا يمكن حصرها بسبب جذري واحد، لكن العصر الرقمي الجديد سيغير تغييراً كلياً اثنين من مثيراتها المعروفة جداً؛ وهما التمييز الممنهج والاضطهاد بحق الأقليات اللذين يجعلان المجتمعات المستهدفة ضحية لعنفٍ مفرط، أو يدفعانها إلى ارتكاب أفعالٍ انتقامية. ونحن نعتقد أن ارتكاب المجازر التي ترقى إلى مستوى الإبادة سيصبح صعباً في المستقبل، أما التمييز فمن المرجح أن يصبح أسوأ وأكثر شخصية. فازدياد التواصلية في

المجتمعات سيزود ممارسي التمييز، سواء أكانوا مجموعات رسمية أو مجموعات يقودها مواطنون، بطرق جديدة تماماً لتهميش الأقليات أو المجموعات غير المرغوب فيها، والتي ستصبح هدفاً أسهل نتيجة استخدامها للتقانة أيضاً.

ستتاح للحكومات المعتادة على قمع الأقليات في العالم المادي مجموعة جديدة تماماً من الخيارات في العالم الافتراضي. وستكون الحكومات التي تدرك كيف تنسق بين سياساتها في كلا العالمين هي الأكثر فعالية في القمع. فإذا نوت حكومة في بلدٍ مزودٍ بالاتصالات مضايقة أقليةٍ معينة في المستقبل، فإنها ستجد عدداً من الإجراءات متاحاً لها بسهولة. وأبسط ما يمكنها فعله هو مسح المحتوى الخاص بالمجموعة عن إنترنت البلاد؛ الأمر الذي سيكون سهلاً على الدول التي تمتلك أنظمة فلترة قوية. فكل ما يتطلبه الأمر هو توجيه مزودات خدمة الإنترنت إلى حجب جميع المواقع التي تحتوي كلمات مفتاحية معينة، وإغلاق المواقع ذات المحتويات الممنوعة. ولإزالة الإشارات الطيارة إلى المجموعة من مواقع مثل فيسبوك ويوتيوب، يمكن للدولة تبنّي سياسة شبيهة بسياسة الصين في الرقابة الفاعلة، حيث يقوم المسؤولون عن الرقابة بإغلاق الاتصال آلياً متى ضبطت كلمة ممنوعة.

من الممكن جداً أن تستهدف الحكومة الصينية أقلية الأويغور في غرب الصين. فلطالما عاشت هذه المجموعة الإثنية - التي تتألف في جلها من مسلمين أتراك، وتتركز في منطقة كزين جيانغ المضطربة - توترات مع قومية الهان الصينية التي تشكل الأكثرية، فالحركات الانفصالية في كزين جيانغ مسؤولة عن مجموعة من التمردات الفاشلة خلال السنوات الأخيرة. وعلى الرغم من صغر أقلية الأويغور، فقد تسببت لبكين بمشاكل لا تحصى، ولن يكون شطحاً في الخيال أن يفكر المرء في أن الحكومة الصينية قد تنتقل من تطبيق الرقابة على أحداث معينة ذات صلة بالأويغور (مثل أعمال الشغب في أورومكي عام 2009) إلى إزالة جميع المحتويات المتعلقة بالأويغور عن الشبكة.

قد ترى الدول في هذا النوع من التصرفات ضرورة سياسية، ومحاولةً للتخفيف من التهديدات الداخلية للاستقرار عبر إزالتها ببساطة. وستبقى المعلومات المتعلقة بالمجموعات متوفرةً خارج البلاد في فضاء الإنترنت بالطبع، لكنها ستختفي داخلياً. وسيكون الهدف من ذلك هو إذلال المجموعة عبر نفي وجودها من أصله، إضافةً إلى عزلها أكثر عن بقية الشعب. وقد تتمتع الدولة بمزيد من الحصانة خلال اضطهاد المجموعة. مع الوقت، إذا كانت الرقابة شاملةً بما يكفي، فإن أجيال المستقبل في مجموعات الأكثرية قد تكبر من دون أية معرفةٍ بالمجموعة الأقلية أو بالقضايا المتعلقة بها. وحذف المحتويات مناورة صامتة يصعب تقدير حجمها، ويستبعد أن تتسبب بإطلاق أجراس الإنذار، لأن مثل هذه الإجراءات سيكون لها أثرٌ حسيٌّ ضئيل، لكنها ستبقى إهانة رمزية ونفسية للمجموعات الأكثر تأثراً. وحتى إذا قدر لحكومة أن بطريقة ما، وظهر أنها تقوم عمداً بحجب محتوياتٍ متعلقة بأقلية ما، فغالباً ما سيبرّر المسؤولون تصرفاتهم بأسباب أمنية، أو سيحيلون الأمر إلى مشاكل فنية وأعطال في البنية التحتية.

إذا أرادت حكومة ما أن تمضي أبعد من مجرد السيطرة على المحتوى، وأن تصعد سياساتها التمييزية لتجعل منها اضطهاداً كاملاً على الشبكة، فبإمكانها إيجاد طرق تحدّ عبرها من إمكانية وصول مجموعةٍ معينة إلى الإنترنت وخدماتها. وقد يبدو ذلك تافهاً إذا قورن بالمضايقات المادية، والاعتقالات العشوائية، والعنف، والتضييق الاقتصادي والسياسي الذي تتعرض له المجموعات المضطهدة في أنحاء العالم اليوم. لكن انتشار الاتصالات وخدمات الإنترنت والخدمات النقالة يوفر منافذ حيوية للأفراد يمكنهم من خلالها تجاوز بيئتهم الراهنة والوصول إلى المعلومات وفرص العمل والموارد والترفيه وإلى أشخاص آخرين. لذا، إن إقصاء الشرائح الاجتماعية المضطهدة من المشاركة في العالم الافتراضي سيكون سياسة قاسية مدمرة، لأنه سيحكم عليها بالعزلة والتخلف، فتصبح عاجزةً عن الوصول إلى فرص النمو والازدهار التي نرى كيف تنشرها الاتصالات في أماكن أخرى. ومع انتقال الصيرفة ومناقلات الرواتب والتسديد على نحو مضطرد إلى المنصات الشبكية، سيؤدي الإقصاء من الإنترنت إلى قصر الإمكانيات الاقتصادية للشعب على نحو خطير، وسيصبح وصول الشخص إلى ماله أو التسديد ببطاقة ائتمانية أو الحصول على قرض أصعب بكثير.

تعمد الحكومة الرومانية منذ اليوم إلى استثناء 2.2 مليون من أبناء الغجر الرومانيين من الفرص المتاحة لبقية الشعب. وقد تجلت سياستها في الفصل في الأنظمة التعليمية وفي الإقصاء الاقتصادي؛ عبر التمييز في التوظيف، وعدم المساواة في الوصول إلى الخدمات الطبية والصحية، ناهيك عن الازدراء الاجتماعي العميق. من الصعب الحصول على إحصاءات تتعلق بمستوى وصول الغجر الرومانيين إلى التقانة اليوم، فالكثيرون منهم يتحاشون تسجيل أنفسهم بهذه الصفة في إحصاءات الحكومة خوفاً من الاضطهاد. لكن، كما أوضحنا سابقاً، سيجد الغجر الرومانيون المتصلون طرقاً يحسنون من خلالها ظروفهم، بل قد يفكرون في المستقبل باعتماد شكل ما من أشكال الدولة الافتراضية.

لكن، إذا قررت الحكومة الرومانية توسيع سياساتها ضد الغجر الرومانيين وتطبيقها في العالم الافتراضي، فستتبخر جميع هذه الفرص تقريباً. قد يتخذ الإقصاء التقاني أشكالاً كثيرة وفقاً لمدى السيطرة التي تتمتع بها الدولة، ومقدار الألم الذي تريد إحداثه. فإذا طلبت من جميع المواطنين تسجيل أجهزتهم وعناوين الإنترنت الخاصة بهم (والكثير من الحكومات تطلب بالفعل تسجيل الأجهزة النقالة)، أو احتفظت بسجل للمتخفين، فسيسهل على السلطات الرومانية باستخدام هذه البيانات أن تحجب وصول الغجر الرومانيين إلى الأخبار وإلى المعلومات الخارجية وإلى المنصات ذات القيمة الاقتصادية والاجتماعية. وسيجد هؤلاء المستخدمون أنفسهم فجأة عاجزين عن الوصول بشكل لائق إلى بياناتهم الشخصية أو إلى خدمات الصيرفة الشبكية الخاصة بهم، حيث ستظهر لهم رسائل خطأ، أو قد يبدو الأمر وكأن سرعات اتصالهم بطيئة ورديئة. وباستخدامها سلطتها على البنية التحتية للاتصالات في البلاد، قد تطلق الحكومة مكالمات هاتفية شكلية لتضغط على الإشارات الهاتفية في أحياء معينة، أو قد تقطع اتصالات الغجر الرومانيين بالإنترنت

من وقت لآخر. وقد تنظم الحكومة - بالتعاون مع موزعين من القطاع الخاص - بيع أجهزة مخترَقة إلى أفراد من الغجر الرومانيين (تباع لهم عبر وسطاء موثوقين من قبلهم ومخترَقين من قبل الحكومة) فتوصل إليهم حواسب محمولة وهواتف نقالة دُست فيها منافذ وأبواب خلفية تسمح للدولة بحقن شيفرات برمجية خبيثة فيها في وقتٍ لاحق. من وقت لآخر، بدلاً من شنّ حملةٍ منظمة لمنع الوصول (من شأنها إثارة تدقيق غير مرغوبٍ فيه)، لن تحتاج الحكومة الرومانية سوى إلى تطبيق عمليات الحجب هذه بشكل عشوائي، لكن بتكرار كاف لإزعاج المجموعة نفسها، وبشكل متقطع يسمح بإنكارها على نحو منطقي. وقد يجد الغجر الرومان بالطبع حلولاً تقانية التفافية غير كاملة تتيح لهم الحد الأدنى من الاتصالات، لكن الحجب قد يكون مدمراً إلى حدٍّ يصبح معه حتى الوصول المتقطع غير كافٍ كبديلٍ لما فُقد. وإذا استمر ذلك لما يكفي من الوقت، فقد تنتهي هذه الدينامية إلى شكل من نظام التمييز العنصري الافتراضي تطبق فيه حزم مختلفة من القيود على اتصالات مجموعات مختلفة ضمن المجتمع.

سيشيع في المستقبل العزل الإلكتروني للأقليات على نحو مضطرد لأن الدول مستعدة لذلك، وهي تمتلك أيضاً البيانات اللازمة. بل إن مثل هذه المبادرات قد تبدأ على شكل برامج حسنة النية تتمتع بدعم شعبـي، لكنها ستتحول مع مرور الوقت إلى سياسات متشددة تأديبية مع تغير السلطة في البلاد. فتخيل على سبيل المثال أن يضغط اليهود الحريديون في إسرائيل لإنشاء ذات قائمة بيضاء لا تتاح فيها سوى مواقع تمت المصادقة عليها مسبقاً، ويتحقق لهم ذلك. فقد يُعتقد في النهاية أن إنشاء زقاق إنترنت خاص بهم لا يختلف عن تشكيل قائمة خاصة من مواقع الإنترنت للأطفال. لكن، إذا شارك اليهود الحريديون بعد ذلك بسنوات في الانتخابات وسيطروا على الحكومة، فسيكون قرارهم الأول ربما هو جعل الإنترنت في إسرائيل برمتها إنترنت كوشر. ومن موقعهم ذاك ستتاح لهم إمكانية الحد أكثر من وصول مجموعات الأقلية ضمن إسرائيل.

النتيجة الأكثر إثارةً للقلق في مثل هذه السياسات هي مدى إضعاف هذه القيود للمجموعات المستهدفة التي قد تتقطع، حرفياً، شرايين حياتها. وإذا كان الوصول المحدود نذيراً بالمضايقات الجسدية أو بعنف الدولة نظراً إلى كونه يعطل قدرة المجموعة على إرسال إشارات الإنذار إلى الخارج، فإنه سينتزع أيضاً من الضحايا قدرتهم على توثيق ما يتعرضون له من إساءة معاملة وتدمير في ما بعد. وسرعان ما سيصبح من الممكن القول إن ما يحدث في خلاءٍ رقمي لا يحدث في الحقيقة.

ستظهر في الدول التي تستهدف حكوماتها مجموعات أقلية أو مجموعات مضطهدة بهذه الطريقة اتفاقات ضمنية أو صريحة بين بعض المواطنين والدولة يقوم الناس وفقاً لها بمقايضة المعلومات أو الولاء بإمكانية وصول أفضل. فالأفراد الذين يبدون تعاوناً ملحوظاً مع الحكومة ستمنحهم الدولة اتصالات أسرع، وأجهزة أفضل، وحماية من المضايقات الشبكية، وطيفاً أوسع من مواقع الإنترنت التي يمكنهم الوصول إليها.

لا ينحصر أي من هذين الإجراءين (حذف المحتويات، أو الحد من الوصول)

بالدول وحدها، إذ يمكن للمجموعات والأفراد ذوي القدرات التقنية تطبيق التمييز الافتراضي بشكل مستقلٍ عن الحكومة. وربما لن ترتكب أول إبادة جماعية افتراضية في العالم على يد حكومة، وإنما على أيدي عصابة من المتعصبين. وقد سبق أن ناقشنا كيف ستلجأ المنظمات المتطرفة إلى نشاطات مدمرة على الشبكة عندما تتطور وتحصِّل المهارات التقانية، وهذا يعني أن بعض هذه النشاطات ستعكس المضايقات المذكورة آنفاً. والأمر نفسه ينطبق على المتطرفين الذين يعملون بمفردهم، فليس من الصعب تخيل ناشط عنيف معادٍ للإسلام يتمتع بمهارات تقانية عالية وهو يلاحق مواقع الوب العائدة للجالية المسلمة المحلية ومنصاتها ومنافذها الإعلامية بهدف مضايقتها. وسيكون ذلك هو المكافئ الافتراضي لتخريب ملكياتها، واقتحام مواقع عملها، والصراخ في وجه أفرادها على ناصيات الشوارع. وإذا كان من يرتكب ذلك متمتعاً بمهارات استثنائية، فسيجد طرقاً تسمح له بالحد من إمكانيات الوصول المتاحة للمسلمين عبر استهداف موجهات معينة تفصلهم عن الإنترنت وتسليط إشارات تشويش على أحيائهم، أو بناء فيروسات حاسب تعطل اتصالاتهم.

سيكون التمييز الافتراضي في الحقيقة أنسب للمتطرفين من الخيارات المتاحة لديهم اليوم. فكما أخبرنا القيادي السابق للنازيين الجدد، والناشط في مجال مكافحة الكراهية حالياً، كريستيان بيتشيوليني: "إن ممارسة الترهيب على الإنترنت من قبل مجموعات الكراهية أو المتطرفين أسهل بكثير؛ لأن الوب يجرد التفاعل من الإنسانية، ويضفي طبقة تغطي الهوية وتحقق الانفصال الافتراضي". ووجود الإنترنت كحجاب على الشخصية، يسهل على المهاجم التفوه بأشياء مؤذية ما كانت لتقال وجهاً لوجه في الأحوال العادية خوفاً من الآخرين أو من الملاحقة. فالخطاب العرقي يحمل - عن استحقاق - وصمة اجتماعية معينة في أعين الشعب بشكل عام. لكن الكلمات على الشبكة يمكن أن تقال من دون أن يربط بينها وبين من يقولها. ويتوقع بيتشيوليني أن تتزايد المضايقات الافتراضية التي تمارسها مجموعات الكراهية بشكلٍ كبير خلال السنوات القادمة لأن "عواقب التمييز على الشبكة تبدو أقل خطورةً على مرتكبها، وبالتالي سيزداد تكرارها وسترتفع درجة حدتها".

كان الإقصاء المادي والقانوني في الماضي هو الإجراء الأكثر استخداماً من قبل الأقوياء في المجتمعات المعرضة للنـزاعات. ونحن نعتقد أن الإقصاء الافتراضي سينضم إلى ذينك الإجراءين (من دون أن يطغى عليهما). وعندما تصبح الظروف لا تطاق - كما يشهد التاريخ - ستنطلق شرارات الصراع.

النزاع متعدد الأبعاد

لطالما كانت المعلومات المضللة والدعاية من المعالم الرئيسة للصراعات البشرية. فروايات يوليوس قيصر الشهيرة عن حروب الغال (بين عام 58-50 ق.م) تعجّ بأخبار القبائل البربرية المتوحشة التي قاتلها. وتحديد الطرف الخير والطرف الشرير في صراع ما مهمة حاسمة، لكنها غالباً ما تكون صعبة في معمعة الروايات

المتنافسة، وستمثل تحدياً أكبر بعد في العصر الرقمي الجديد. فحروب التسويق بين المجموعات ستصبح في المستقبل سمة ملازمة للنـزاعات؛ لأن جميع الأطراف ستجد بين أيديها المنصات والأدوات والأجهزة الكفيلة بتحسين قدرتها على رواية القصص على مسامع الجمهور في الوطن وفي الخارج. وقد رأينا ذلك يتكشّف في شهر تشرين الثاني عام 2012 خلال الصراع بين إسرائيل وحماس، عندما شنت حماس حرب تسويق شاملة أغرقت العالم الافتراضي بصور لنساء وأطفال أموات. وتمكنت حماس، التي تعتمد على جمهورٍ يائس، من استغلال عدد الوفيات الأكبر في غزة. وردت إسرائيل، التي تركز أكثر على إدارة المعنويات الوطنية وإزالة الغموض الذي يكتنف تصرفاتها، باستخدام عنوان تويتر IDFSpokesperson@ لتبث عبره تغريدات مثل "فيديو: طيارو الجيش الإسرائيلي ينتظرون إخلاء المنطقة من المدنيين قبل ضرب الهدف"، يليه عنوان فيديو على يوتيوب. لكن واقع حروب التسويق يقول إن الجهة التي تنقل أحداث القتل والموت واستخدامه في دعايتها غالباً ما تنال قدراً أوسع من التعاطف، خصوصاً حين ينضم جمهورٌ أعرض إلى الحديث. فما من شيءٍ جديد في إجراءات حماس الدعائية، لكن الانتشار المتنامي لمنصاتٍ مثل يوتيوب وفيسبوك وتويتر مكّنها من الوصول إلى جمهورٍ أعرض بكثير في الغرب غير ناطق بالعربية كان يضخم حرب حماس التسويقية مع كل تغريدةٍ وكل إعجابٍ.

ستسعى المجموعات المتصارعة إلى تدمير القدرات التسويقية الرقمية لبعضها بعضاً؛ حتى قبل أن يبدأ الصراع. قليلةٌ هي الصراعات التي تنتهي إلى فصلٍ واضح بين الأبيض والأسود في خاتمتها (ناهيك عن بدايتها)، وسيكون لشبه التكافؤ في قوة الاتصالات على هذا النحو تأثيرٌ كبير على تعاطي المدنيين والقادة والعسكريين مع الصراع. بل وأكثر من ذلك، فإن حقيقة أن الجميع قادرون على إنتاج ترجمتهم للأحداث ومشاركتها ستؤدي إلى إبطال الكثير من المزاعم. فمع وجود الكثير من الروايات المتضاربة، ومن دون طريقة للتحققٍ تكون ذات مصداقية، ستفقد جميع الادعاءات قيمتها، وستأتي إدارة البيانات (أي ترجمتها وفهرستها وتصنيفها والتحقق من المحتويات القادمة من مناطق الصراع) في الحرب، التحدي الرئيس الثاني، بعد تحدي إتاحة التقانة مباشرةً.

تمكن تقانات الاتصالات الحديثة الضحايا والمعتدين في صراعٍ معين على حدٍّ سواء من إضفاء الشك على رواية الطرف الآخر على نحوٍ أكثر إقناعاً من أية وسيلة عرفها التاريخ. وربما تكون جودة تسويق الدول لنفسها هي العامل الوحيد الذي يفصل بين بقائها في السلطة ووقوعها فريسة تدخلٍ أجنبـي. أما بالنسبة إلى المدنيين العالقين في حصارٍ على مدينةٍ من قبل قوى الحكومة، فيمكنهم مواجهة ادعاءات الدولة بواسطة مقاطع فيديو الهواة القوية، والربط بالزمن الحقيقي مع الخرائط الفضائية، بما يدل بشكلٍ قوي - بل قد يكفي كبرهان - على أنها تكذب. إلا أنه في حالاتٍ معينة، كأعمال العنف في ساحل العاج عام 2011 (حين تورط الطرفان في معركة عنيفة بسبب نتائج الانتخابات المختلف عليها) حيث كان الطرفان يتمتعان بتسويقٍ رقمي جيد على المستوى نفسه، يصبح من الصعب تبين

ما يحدث بالفعل. وحين لا يكون أي من الجانبين مسيطراً تماماً على تسويقه (أي عندما يقوم أفراد متحمسون من خارج القيادة المركزية بإنتاج محتوياتهم الخاصة) يرتفع مستوى الإبهام أكثر بعد.

أما بالنسبة إلى المراقبين الخارجيين، فإن الأسئلة التي كانت صعبةً أصلاً، مثل تحديد من عليهم أن يتحدثوا معه لفهم الصراع، أو إلى جانب من عليهم الوقوف، وما هي أفضل طريقة لتقديم الدعم، تزداد تعقيداً على نحو لا يستهان به في عصر حروب التسويق (وهي الحال تحديداً عندما يكون قلة من المراقبين الخارجيين قادرين على تحدث اللغة المحلية، أو في غياب تحالفات رسمية بين بلدان الناتو وبلدان جمعية التنمية الأفريقية الجنوبية "سادك" مثلاً). وستدفن المعلومات، الحاسمة في عملية اتخاذ القرار في هذه المسائل، تحت أكوام من المحتويات المنحازة والمتضاربة الصادرة عن منطقة الصراع. والدول نادراً ما تتدخل عسكرياً قبل أن تتبين تماماً ما الذي يحدث. وحتى عند ذلك، نجدها تتردد خوفاً من العواقب المادية غير المحسوبة ومن التدقيقات التي ستجريها دورة الأخبار الجارية على مدار الساعة.

ستكون لحروب التسويق الدائرة حول نـزاعٍ في الخارج آثارها السياسية المحلية أيضاً، فإذا تأثر معظم الجمهور الأمريكي بمقاطع فيديو مشحونة عاطفياً تعود لطرف واحد، وارتأى أن التدخل في صراعٍ معين يمثل ضرورةً أخلاقية، بينما تقترح استخبارات حكومة الولايات المتحدة أن هذه الأفلام لا تمثل انعكاساً للديناميات الحقيقية في الصراع، فكيف يمكن للإدارة أن تستجيب؟ إذ لا يمكنها الكشف عن مواد سرية لتبرير موقفها، ولا يمكنها أن تواجه على نحوٍ فعال الرواية التي يعتمدها الجمهور. فعندما يقدم كلا الطرفين نسختين للأحداث بالمستوى نفسه من الإقناع يجمد الفاعلون الخارجيون في أماكنهم عاجزين عن اتخاذ أي خطوة في أي اتجاه. وهو ما قد يكون بالضبط ما يسعى إليه أحد طرفي الصراع.

ستبدأ حروب التسويق في المجتمعات المعرضة للعنف الإثني والطائفي قبل اندلاع الشرارة التي تشعل اقتتالاً حقيقياً بوقت طويل عادة. فكثيراً ما يتم تضخيم المظالم التاريخية واختلاقها مع الاتصالات في الفضاء الافتراضي كما بيّنا سابقاً. فهذه الاتصالات قد تقوي وجهات النظر المتضاربة بدلاً من أن تشذب العلات التي تعتري دقتها. وقد تتأجج التوترات الطائفية - التي ظلت لسنواتٍ طويلة خامدةً نوعاً ما - مجدداً عندما يتاح للناس وسطٌ شبكي مغفل الهوية. وقد سبق لنا أن رأينا كيف يمكن للحساسيات الدينية أن تشتعل بشكلٍ فوري تقريباً عندما يصل خطاب، أو صور مثيرة للجدل، إلى الإنترنت (وليست الرسوم الدانماركية المثيرة للجدل عام 20، والمظاهرات العنيفة ضد فيلم براءة المسلمين عام 2012 سوى غيضٍ من فيض). لذا، لا مفر من أن الفضاء الشبكي سيمنح الناس طرقاً أكثر يهينون بها بعضهم. والطبيعة الفيروسية لانتشار المحتويات المثيرة للفتن لن تدع أي فعلٍ سيئ في أي جزء من العالم يمر مرور الكرام.

إن التسويق شيء والاستخبارات شيء آخر بالطبع. إذ ستكون محاولات التسويق الرقمي المبكرة التي تقوم بها مجموعات متصارعة مجرد دعاية فظّة

ومعلومات مضللة انتقلت إلى منصة افتراضية. لكن، مع تبني الدول والأفراد حول العالم هذه السلوكيات، ستضيق مع الوقت المسافة الجمالية القائمة بين الاستخبارات والتسويق، وسيترتب على الدول توخي الحذر لعدم الخلط بين الاثنين. فعندما تدرك المجموعات ما ينقصها لتحريض رد فعل معين، ستتمكن من تخصيص محتوياتها ورسائلها بالشكل المناسب*.

ستكون لأولئك الذين يملكون موارد على مستوى الدولة اليد العليا في حرب التسويق، لكنهم لن يحتكروا التفوق في أي حالٍ من الأحوال. فحتى مع سيطرة الدولة على الكثير من وسائل الإنتاج (من أبراجٍ خلوية، ووسائل إعلام حكومية، ومزودات خدمة إنترنت) سيستحيل على أي طرفٍ أن يحقق احتكاراً كاملاً للمعلومات. وإذا كان تصميم محتويات المستخدمين وتحريرها وتحميلها ونشرها لا يتطلب سوى هاتف بحجم الكف، فلن يكون بإمكان النظام أن يهيمن تماماً. فمقطع الفيديو الذي صورته كاميرا هاتف نقال مرتعشة خلال الاحتجاجات التي تلت الانتخابات في إيران هيج حركة المعارضة؛ ونقصد هنا فيديو ندى الشهير. وندى آغا سلطان شابة تعيش في طهران كانت قد ركنت سيارتها على جانبٍ هادئ من الشارع خلال احتجاجات معاديةٍ للحكومة، وكانت قد خرجت من سيارتها تفادياً للحر، فأصيبت برصاصةٍ في قلبها أطلقها قناص من أحد الأسطح القريبة. وكان من المدهش أن المشهد برمته قد تم تصويره بواسطة هاتف نقال لشخص ما. فبينما كان بعض المتجمهرين يحاولون إسعاف ندى، بدأ آخرون بتصويرها على هواتفهم أيضاً، وصارت مقاطع الفيديو تتنقل بين أيدي الإيرانيين عبر منصات بلوتوث ثنائية في أغلب الأحيان، بعد أن قام النظام بحجب الاتصالات النقالة تحسباً للاحتجاجات. وسرعان ما وجدت طريقها إلى الإنترنت، وبدأ انتشارها الفيروسي، فتحمّس المراقبون حول العالم، وراحوا يشجبون النظام الإيراني، فيما انطلقت الاحتجاجات في إيران منادية بالقصاص لندى. وأدى كل ذلك إلى زيادة الاهتمام العالمي إلى حدٍّ كبير بحركة الاحتجاجات التي كان النظام يستميت لإيقافها.

حتى في أكثر المجتمعات تقيداً، وفي الأماكن التي تتفشى فيها برمجيات التجسس والمضايقات الافتراضية والهواتف النقالة المخترقة سلفاً، سيجد أفراد عاقدو العزم طريقة لإيصال رسائلهم إلى الخارج. وقد يكون من بين تلك الطرق تهريب بطاقات سيم وإعداد الشبكات التعشيقية (والتي تتألف بشكل أساسي من مجموعة من الأجهزة اللاسلكية التي تلعب جميعها دور الموجهات، حيث تنشئ عقداً متعددة لنقل البيانات بدلاً من وجود جهازٍ محوري مركزي)، أو توزيع هواتف

مصممة بطريقة لا تتيح لها تسجيل أية اتصالات (عبر جعل جميع المكالمات تجرى من خلال تقنية الصوت على الآي.بـي مثلاً)، والتي تسمح باستخدام خدمات الإنترنت مع إغفال الهوية. وستصاب جميع محاولات الدولة للحد من انتشار تقانة ما مرغوبة بالفشل، فانتشارها مسألة وقت فقط (وينطبق ذلك حتى على الأقليات المضطهدة التي تحاول الحكومة إقصاءها من الإنترنت). فقبل فيديو ندى بوقت طويل، حاولت إيران منع صحون التلفزة الفضائية، وجاء الرد على وصايتها على شكل انتشارٍ أكبر لهذه الصحون لدى الجمهور الإيراني. بل وتعتبر

سوق الصحون الفضائية غير الشرعية في إيران إحدى أكبر هذه الأسواق مقارنةً بعدد السكان في العالم، بل إن بعض عناصر النظام يتربحون من مبيعات هذه السوق.

تبين الإبادة الجماعية التي حدثت في رواندا عام 1994، والتي نتجت عن أحد أبرز نـزاعات العصر ما قبل الرقمي وحصدت أرواح 800 ألف من البشر، الفرق الذي يحدثه التناسب في القدرة التسويقية. ففي عام 1994، وبينما كانت أجهزة الراديو متوفرة لدى الهوتو والتوتسي والتوا على حدٍّ سواء، كان الهوتو هم الوحيدين الذين يمتلكون محطاتٍ إذاعية. ومع افتقار التوتسي للوسائل التي تعلي أصواتهم، وقفوا عاجزين أمام سيل من الدعاية وخطاب الكراهية المتدفق عبر موجات الأثير. وعندما حاول التوتسي تشغيل محطة إذاعتهم الخاصة تعرفت الحكومة التي يسيطر عليها الهوتو على مشغلي المحطة وأغارت على مكاتبهم واعتقلت بعضهم. لكن، لو كانت أقلية التوتسي تمتلك الأجهزة النقالة الفعالة التي نمتلكها اليوم في السنوات التي سبقت إبادة عام 1994، لربما تمكنت من التشكيك في الخطاب العام في رواندا، ولما وجد مدنيو الهوتو العاديون في الدعاية المعادية للتوتسي ما يكفي لإقناعهم ولدفعهم إلى حمل السلاح ضد إخوانهم الروانديين، ولتمكن التوتسي من نشر محتوياتهم الخاصة من أجهزتهم المحمولة أثناء تنقلهم من دون أن يضطروا للاعتماد على موافقة الحكومة أو الوسطاء على تطوير محتويات ونشرها. ففي فترة الإبادة، كانت محطات راديو الهوتو تعلن أسماء وعناوين الأشخاص المتخفين. وليس من الصعب تخيل الفرق الذي كان يمكن أن تحدثه قناة اتصالات بديلة؛ كخدمة تراسل مشفرة ثنائية مثلاً.

بالرغم من المكاسب الممكن تحقيقها، ستبقى هناك عواقب طويلة المدى لميدان اللعب الجديد المستوي، رغم أننا لا نستطيع توقع ما سنفتقده عندما تزال الحواجز التقليدية. فالمعلومات المضللة، كما ذكرنا آنفاً، ستتسبب بتشتيت التركيز وبالتشويه؛ مما سيدفع جميع الأطراف إلى إساءة تفسير الأحداث وإساءة تقدير الرد المناسب. فليست كل جريمةٍ وحشية ترتكب جزءاً من مذبحة منظمة بحق مجموعة إثنية أو دينية. إلا أنه من الممكن إلباسها هذا الثوب المزيف بقليل من الجهد. ولما كان التضليل بالمعلومات مشكلةً كبرى حتى ضمن ظروفٍ محلية، فكيف يمكن لحكومةٍ محلية أن تتعامل مع جمهورٍ غاضب يكتسح مكاتب البلدية مطالباً بالقصاص بسبب فيديو تم التلاعب به؟ ستواجه الحكومات والسلطات أسئلة مثل هذه بشكلٍ متكرر، ولن تتمكن من إعطاء سوى القليل من الأجوبة المرضية.

إن الرد الأفضل، وربما الوحيد، على هذه التحديات يتمثل بالتحقق الرقمي. فالتحقق من تعرض صورةٍ إلى التلاعب (عبر التحقق من العلامة المائية الرقمية) أو ملف فيديو للتحرير الانتقائي (عبر التعهيد الجماعي للمقطع كله، وإثبات ضياع أجزاء منه، أو أن شخصاً ما عرض أنه ميت بينما هو في الحقيقة لا يزال على قيد الحياة؛ وذلك عبر تتبع هويته على الشبكة)، سيضفي بعض المصداقية على النـزاع فائق الاتصال. وسيكون بإمكان شاهد على هجومٍ للميليشيات في جنوب السودان

في المستقبل أن يضيف أشياء مثل العلامات المائية الرقمية، والبيانات البيومترية، وإحداثيات الموقع المحددة بالأقمار الصناعية، لتدعيم ادعاءاته. وسيكون ذلك مفيداً عندما يشارك محتواه مع الشرطة ومع وسائل الإعلام. فالتحقق الرقمي هو المرحلة التالية في هذه العملية بلا شك، وهو يتم بالفعل عندما يقوم الصحفيون والمسؤولون الحككوميون بمقاطعة مصادرهم مع أشكال أخرى من المعلومات، وسيصبح أسهل بعد، وأكثر مصداقيةً، عندما تنجز الحواسب معظم العمل.

من الممكن تشكيل فرق من مراقبـي التحقق الدوليين وإرسالهم إلى مناطق النـزاع التي تظهر فيها خلافات كبيرة حول الروايات الرقمية. وعلى غرار الصليب الأحمر، سيتم إرسال مراقبـي التحقق كوكلاء حياديين، لكنهم سيكونون في هذه الحالة على قدر عال من التأهيل التقني*. (وليس من الضروري أن يتم إرسالهم إلى مناطق الصراع الفعلية في جميع الحالات، حيث يمكنهم أحياناً إنجاز عملهم عبر الإنترنت. أما في الصراعات التي تكون فيها البنية التحتية للاتصالات محدودة أو واقعةً تحت سيطرة أحد الأطراف، فسيكون من الضروري أن يتواجدوا على مقربة من الفاعلين، وأن يتمتعوا بالمهارات اللغوية وبالمعرفة الثقافية اللازمة). وسيكون تصديقهم ذا قيمة عالية، إذ سيكون بمثابة الضوء الأخضر لوسائل الإعلام وغيرها من المراقبين لأخذ هذه المحتويات على محمل الجد. وقد تتمكن دولة ما أو أحد أطراف النـزاع من تجاوز هؤلاء المراقبين، لكن ذلك سيحط من قيمة أية محتويات تنتجها، وسيضعها موضع شك كبير في عيون الآخرين.

سيقوم هؤلاء المراقبون بالتحقق من البيانات، وليس من الأفعال. وسيكون للنتائج التي يتوصلون إليها وزن كبير، فعلى أساسها قد تقرر دولٌ التدخل أو إرسال مساعدات أو فرض عقوبات بناء على ما يقولون. ومع كل هذه الثقة والمسؤولية تأتي بالطبع إمكانية إساءة الاستخدام التي لا يمكن تجنبها؛ بما أن هؤلاء المراقبين لن يكونوا أكثر مناعة على الفساد الذي يحرج المنظمات الدولية الأخرى. وقد تسعى الأنظمة إلى كسب مراقبـي التحقق عبر الرشى أو الابتزاز، كما أن بعض المراقبين قد يُضمروا بعض التحيز الذي لا ينكشف سوى بعد فوات الأوان. وبغض النظر عن كل ذلك، إنّ معظم هؤلاء المراقبين سيكونون من المهندسين والصحفيين الشرفاء الذين سيتعاونون معاً، والذين سيقود حضورهم في أي نـزاع إلى المزيد من الأمان والشفافية لجميع الأطراف.

حين لا تنخرط المجموعات المتنازعة في حروب التسويق، فإنها ستهاجم أية كيانات على الشبكة تعتبرها ذات قيمة للطرف الآخر. أي إنها ستهاجم مواقع الوب، والمنصات، والبنية التحتية للاتصالات التي تتمتع بأهمية استراتيجية أو رمزية ما؛ عبر هجمات حجب الخدمة الموزعة والفيروسات المتطورة وجميع أنواع الأسلحة الافتراضية. وستصبح الهجمات الشبكية جزءاً متكاملاً من المنهجية التكتيكية للمجموعات المتنازعة، سواء أكانت منخرطة في معركة خفيفة أم في حرب كاملة الصفات. فمهاجمة شبكة الاتصالات العائدة لمجموعة منافسة وإضعافها لن يؤثرا فقط على قدراتها على التسويق الرقمي، بل وعلى الموارد والمعلومات المتاحة أمامها، وعلى القاعدة الداعمة لها أيضاً. وما إن يتم النيل من الشبكة أو قاعدة

البيانات بنجاح حتى تتمكن المجموعة المتسللة من استخدام المعلومات التي جمعتها لكي تبقى على اطلاع، ولكي تنشر المعلومات المضللة وتشنّ الهجمات الوقائية، بل ولتتعقب الأهداف عالية القيمة (إذا وجدت مجموعة أرقام الهواتف النقالة لمسؤولين في النظام على سبيل المثال، واستخدمت برمجيات مراقبة تكشف عن مواقعهم).

ستشن الهجمات الافتراضية بشكل مستقل أو أخذاً بالثأر. فإذا فقد أحد طرفي حرب أهلية منطقة على سبيل المثال، فقد يثأر بأن يوقف مواقع الوب التي يستخدمها خصمه لدعايته، حيث يحد من قدرته على التباهي بانتصاره. وهو بالطبع ليس مكسباً مكافئاً لما فقده، لكنه يبقى مؤذياً. وسيكون ذلك في العالم الافتراضي بمثابة قصف وزارة الإعلام التي غالباً ما تكون من بين الأهداف الأولى في النـزاعات في العالم المادي. وستتمكن حكومة قمعية من تحديد البوابات المالية الشبكية التي يستخدمها الثوار في بلادها لتلقي التمويل من داعميهم في الشتات وتدميرها. وسيأخذ القراصنة المتعاطفون مع هذا الجانب أو ذاك على عاتقهم تفكيك أي شيء يمكنهم الوصول إليه، كقنوات يوتيوب التي يشغلها الخصوم وقواعد البيانات التي تهم الطرف الآخر. فعندما بدأ الناتو عملياته العسكرية في صربيا عام 1999، استهدف قراصنة مناصرون للصرب مواقع وب عامة تعود إلى كل من الناتو ووزارة الدفاع الأميركية محققين بعض النجاح (أصبح موقع الشؤون العامة لكوسوفو العائد للناتو "غير قابل للتشغيل عملياً" طوال أيام نتيجة لهذه الهجمات التي عرقلت أيضاً مخدم البريد الإلكتروني العائد للمنظمة).

سنشهد خلال العقود القادمة أول حركة تمرد في العالم. وستحتاج هذه الحركة بالتأكيد إلى السلاح والبشر لتحدي الحكومة، لكن المتمردين سيكونون مسلحين بالتقنيات وبلائحة أولويات تملي أسلوباً جديداً. فحتى قبل أن يعلنوا عن حملتهم، قد يقومون باستهداف شبكة الاتصالات التابعة للحكومة إدراكاً منهم لكونها تشكل العمود الفقري الحقيقي (وإن لم يكن رسمياً) لدفاعات الدولة. وربما يتواصلون سراً مع حكومات متعاطفة معهم للحصول على المكونات التقنية الضرورية (من ديدان وفيروسات ومعلومات بيومترية) لتعطيل هذه الشبكة من الداخل أو من الخارج. ويمكن من خلال هجوم يستهدف البنية التحتية للاتصالات أن تؤخذ الحكومة على حين غرة. وطالما أن المتمرّدين لم يقوموا هجومهم، فسيبقى للحكومة أن تستغرب وتتساءل عن مصدر الهجوم ومن يقف وراءه. وقد يترك المتمردون إشارات مزيفة تشير إلى مصدر الهجوم، وربما تشير إلى أحد الأعداء الخارجيين للدولة؛ لتحقيق المزيد من الاضطراب. وبينما تعمل الدولة على استعادة حضورها على الشبكة، ربما يضرب المتمردون مرة أخرى متسللين هذه المرة إلى شبكة الإنترنت العائدة للحكومة، ومنتحلين شخصيات أخرى (حيث يخدعون الشبكة ويجعلونها تعتقد أن المتسللين مستخدمون شرعيون) لتحقيق مزيد من التشتت، ولتعطيل عمليات الشبكة (وإذا تمكن المتمردون من الوصول إلى قاعدة بيانات بيومترية هامة، فسيتمكنون من سرقة هويات مسؤولين حكوميين وتقمصها على الشبكة للإدلاء بتصريحات مزيفة أو القيام بعمليات شراء

مشبوهة). وقد يستهدف المتمردون في النهاية شيئاً مادياً، كشبكة الطاقة في البلاد التي سيؤدي التلاعب بها إلى غضب شعبـي يُصبُّ جامه من غير حق على الحكومة. وهكذا، قد تجد الحركة المتمردة الذكية نفسها عبر ثلاث هجمات رقمية، ومن دون إطلاق رصاصة واحدة في موقع يسمح لها وحدها بتعبئة الجماهير ضد الحكومة التي لم يكن لديها أدنى علم بالتمرد المحلي. ويمكن للمتمردين عند هذه المرحلة البدء بهجومهم العسكري وفتح جبهة ثانية مادية.

ستتأثر النـزاعات في المستقبل أيضاً بنـزعتين واضحتين وإيجابيتين بشكل عام تفرضهما الاتصالات، أولاهما هي الحكمة التي تتمتع بها الجماهير على الشبكة، والثانية هي ديمومة البيانات بوصفها دليلاً يصعب على مرتكبـي العنف - كما أسلفنا - بفضلها إنكار جرائمهم أو التقليل من شأنها.

تمثل الحكمة الجماعية على الإنترنت موضوعا شائكاً. فالكثيرون ينتقدون بشدة الحالات السلبية المتطرفة للتعاون على الشبكة، مثل (أي إجماع مجموعة من مجموعات المستخدمين على الإنترنت) الرديء جداً، أو الخبث الذي ينطوي عليه السلوك الزُمَري الذي يغذيه إغفال الهوية على المنتديات والشبكات الاجتماعية وغيرها من القنوات على الإنترنت. بينما يحتفي البعض بالمستوى الذي تحققه منصات المعلومات التي تعتمد على التعهيد الجماهيري، مثل ويكيبيديا، من الدقة والموثوقية. وأياً كان رأيك، ستبقى هناك مكاسب محتملة يمكن للحكمة الجمعية أن تقدمها في نـزاعات المستقبل.

عندما تتساوى الفرص المتاحة أمام جميع أطراف الصراع من ناحية المعلومات، يصبح بمقدور عدد أكبر من المواطنين المساهمة في صياغة الروايات التي تظهر. وسيضمن الانتشار الواسع للهواتف النقالة أن يطلع عدد أكبر من الناس على ما يحدث داخل البلاد مقارنة بأوقات خلت. وسيوسع الاتصال بالإنترنت نطاق المشاركة ليضم طيفاً واسعاً من الفاعلين الخارجيين. وبالإجمال، سيكون هناك دائماً عدد من الناس على طرف الخير أكثر منهم على جانب المعتدي. وبوجود شعب ملتزم، ثمة فرصة أفضل لتعبئة المواطنين ضد الظلم أو الدعاية، فحين يغضب عدد كاف من الناس بسبب ما يرونه، فإنهم يجدون القنوات التي يجعلون أصواتهم مسموعة من خلالها. ويمكنهم التصرف فرادى أو جماعات، حتى لو كان ذلك الغضب - كما رأينا في سنغافورة - سببه الطبخ بالكاري.

إن التحديات التي ينطوي عليها ضبط الإنترنت قد تؤدي أيضاً إلى خطر الاقتصاص غير القانوني على الشبكة كما تبيّن لنا قصة محركات بحث اللحم البشري في الصين: (رنرو سوسو يين كينغ). فوفقاً لمقالة توم دوني الملهمة الصادرة في آذار عام 2010 في مجلة نيويورك تايمز، ظهرت في الصين قبل ذلك بسنوات نـزعة مقلقة في الفضاء الشبكي للصين، فكانت أعداد غفيرة من مستخدمي الإنترنت تنتقي أفراداً ممن أثاروا غضبها وتتعقبهم وتضايقهم (وما من منصة مركزية للقيام بهذا الفعل، كما لا يمكن حصر هذه النـزعة بالصين، لكن هذه الظاهرة أكثر ما تعرف وتفهم هناك بفضل سلسلة من الأمثلة البارزة). ففي عام 2 راج مقطع فيديو مريع على منتديات الإنترنت الصينية تظهر فيه امرأة وهي تدهس

بحذائها ذي الكعب العالي قطة صغيرة حتى الموت، فتم البحث عن الفاعلة على مستوى البلاد. وبفضل أعمال تحقيق مجتهدة على مستوى جماهيري، سرعان ما تم اقتفاء أثر الفاعلة والعثور عليها في بلدة صغيرة في شمال شرق الصين. وبعد نشر اسمها ورقم هاتفها ومكان عملها على الملأ، كان عليها أن تهرب هي ومصورها. فليست الحواسب وحدها هي القادرة على إيجاد إبرة في كومة من القش على ما يبدو، إذ لم يستغرق العثور على هذه المرأة من بين أكثر من مليار صيني (واعتماداً على الأدلة التي يحملها الفيديو فقط) سوى ستة أيام.

يمكن لهذا السلوك الجماهيري أن ينحرف ليتحول إلى فوضى لا يمكن توقع عواقبها. لكن هذا لا يعني التخلي عما يحمل ثمار الطاقة الجماعية من أجل الخير. فتخيل لو كان الهدف النهائي للمستخدمين الصينيين ليس مضايقة قاتلة القطة وإنما إحضارها إلى العدالة عبر القنوات الرسمية. ففي سياق صراع ما، حين تكون المؤسسات منهارة، أو حين تفقد ثقة الشعب، من شأن الطاقة الجماهيرية إنتاج معلومات أكثر شمولاً ودقة تساعد على ملاحقة المجرمين المطلوبين، وعلى رفع المطالب بالمحاسبة؛ حتى في أصعب الظروف.

لكن أهمية العدالة التي تتعهدها الجماهير تصبح حاسمة إذا اقترنت بتطور آخر؛ ألا وهو ديمومة البيانات. فالكشف عن الفظاعات بزمن حقيقي، وأمام جمهور علني أمر ضروري، وكذلك حفظها بشكل دائم وتمكين أي شخص يريد الإشارة إليها (سواء أكان الهدف هو الملاحقة القضائية أو التشريع أو دراستها لاحقاً). وقد يكون للحكومات - ومعتدين غيرها - التفوق العسكري عبر الأسلحة والدبابات والطائرات، لكن المعركة التي ستخوضها ضد الآثار المعلوماتية التي ستخلفها وراءها ستكون معركة عسيرة عليها. فعندما تحاول حكومة حجب الاتصال عن مواطنيها، ربما ستتمكن من إخفاء بعض الأدلة التي يتم تناقلها عبر البلاد وخارجها، لكن هذا الدفق سيستمر. والأهم من ذلك أن وجود هذا الدليل - وإن كان محطاً للجدل في وقته - سيؤثر على طريقة معالجة الصراع، وعلى خاتمته، وعلى الطريقة التي سينظر بها إليه لوقت طويل في المستقبل.

المحاسبة، أو التهديد بها فكرة فعالة، وهذا هو السبب الذي يدفع الناس إلى تدمير الأدلة. ففي غياب البيانات الملموسة، قد تعيق الروايات المتضاربة العدالة وتمنع الوصول إلى نتيجة في النهاية. وينطبق ذلك على المواطنين والدول على حدٍّ سواء، ففي شهر كانون الثاني عام 2012 اختلفت فرنسا وتركيا دبلوماسياً عندما مرر مجلس الشيوخ الفرنسي قانوناً (أسقطه بعد شهر واحد المجلس الدستوري الفرنسي) يجرِّم إسقاط صفة الإبادة الجماعية عن القتل الجماعي الذي ارتكب بحق الأرمن من قبل الإمبراطورية العثمانية عام 1915. ولكن الحكومة التركية، التي ترفض مصطلح وتدعي أن عدد الأرمن الذين قتلوا أقل بكثير من 1.5 مليون، اعتبرت القانون ، وقالت إن الحكم على عمليات القتل يجب أن يترك للمؤرخين. لكن توفر الأجهزة التقانية والمنصات وقواعد البيانات التي نمتلكها اليوم سيجعل من الصعب جداً على الحكومات في المستقبل أن تحاجج بادعاءات كهذه. ليس فقط بفضل ديمومة الأدلة، بل أيضاً لأن أي شخص آخر

سيكون قادراً على الوصول إلى المواد المصدرية نفسها.

ستتوفر في المستقبل أدوات - كمقارنة البيانات البيومترية، وتتبع بطاقات السيم، ومنصات توليد المحتويات سهلة الاستخدام - ستصل من خلالها إمكانية المحاسبة إلى مستوى لم تصله من قبل. حيث سيكون بإمكان شاهد على جريمة أن يستخدم هاتفه لتصوير ما يراه، وأن يتعرف على المعتدي وعلى الضحية بواسطة برمجيات التعرف على الوجوه بشكل شبه لحظي من دون أن يضطر لتعريض نفسه للخطر بأي طريقة. وسيتم تحميل المعلومات المتعلقة بالجرائم أو الأعمال الوحشية في صيغة رقمية - وبشكل آلي - إلى السحابة (مما يمنع فقدان أية بيانات إذا صودر هاتف الشاهد)، وربما يتم إرسالها إلى هيئة مراقبة أو هيئة قضائية دولية. ويمكن لمحكمة دولية عندئذ أن تجري تحقيقاتها، وأن تبدأ - وفقاً لما تجده - محاكمة علنية افتراضية تبث مرافعاتها في البلاد التي يطوفها الجاني حراً طليقاً. وإذا لم يكف خطر العار العلني والتهم الجنائية لردع القادة، فسيكفي لجعل الجنود البسطاء يفكرون ملياً قبل الانخراط في نشاطات عنفية. وستتوفر أدلة تم التحقق منها تحققاً احترافياً على موقع وب لاهاي قبل المحاكمة، وسيكون بوسع الشهود أن يدلوا بشهاداتهم افتراضياً وهم في مأمن.

إن عجلات العدالة بطيئة في دورانها بالطبع، وخصوصاً في متاهة القانون الدولي. وخلال تطوير نظام يضمن سرعة استجابة البيانات، سيتم تحقيق مكاسب وسيطة تتمثل بتخزين الأدلة القابلة للتحقق، وستكون النتيجة هي تطبيق القانون بشكل أفضل، حيث يمكن لتطبيق مفتوح المصدر تعده المحكمة الجنائية الدولية أو هيئة أخرى أن يظهر أهم المجرمين المطلوبين في العالم مقسمين حسب البلد. وتماماً كما تستطيع محركات بحث اللحم البشري الصينية الإشارة إلى شخصٍ ما وتحديد موقعه وتفاصيل معلومات الاتصال الخاصة به، يمكن توجيه هذه القدرة نفسها لتصيد المجرمين (تذكر أنه ستتوفر بين أيدي الناس هواتف أشدّ فعالية حتى في أقصى الأماكن). وباستخدام المنصة نفسها، يمكن للمواطنين المهتمين بالأمر حول العالم المساهمة مالياً لجمع مكافأة كحافز لإلقاء القبض على الشخص المطلوب. عندها، بدلاً من أن يواجه المجرم القصاص الجماهيري، سيتم إلقاء القبض عليه من قبل الشرطة وتقديمه للمحاكمة.

ستقيم الطاقة الجمعية للعالم الافتراضي حاجزاً هائلاً أمام المتورطين المحتملين في الأعمال الوحشية والممارسات الفاسدة؛ بل وحتى الجرائم ضد الإنسانية. ولا شك في أنه ستبقى هناك دائماً نوعيات خبيثة حقاً لن ينفع معها الردع، لكن الأفراد ذوي السلوك المنحرف فقط سيجدون التكاليف المحتملة للسلوك السيئ في العصر الرقمي أعلى مع الوقت. فبعيداً عن احتمال تعرّضهم للمحاسبة الكبير، وإمكانية توثيق الجريمة والاحتفاظ بوثائقها إلى الأبد، سيستخدم المراقبون التقانة للوصول إلى أعرض جمهور ممكن، وسيكون للمرتدّين دافع أكبر بكثير لتجنب الاتهامات بالتورط في هذه الجرائم الموثقة أيضاً. وربما يتم بناء برنامج حماية شهود رقمي يزود المخبرين بهويات افتراضية جديدة (كتلك التي يتم بيعها في الأسواق السوداء كما ذكرنا سابقاً) لمنحهم دوافع أكبر للمشاركة.

سيساعد توفر الأدلة الرقمية الدائمة على إقامة العدالة في المرحلة الانتقالية بعد انتهاء الصراع. وستعتمد لجان الحقيقة والمصالحة في المستقبل على مجموعة من السجلات الرقمية والمشاهدات الفضائية والفيديوهات وصور الهواة وتقارير التشريح والشهادات (سنأتي على شرح هذا الموضوع باختصار). ومرة أخرى، سيكون الخوف من الإدانة رادعاً كافياً بالنسبة إلى بعض المتورطين المحتملين الذين ربما سيخففون على الأقل من مستوى العنف.

بعيداً عن توثيق الفظاعات، ستلعب ديمومة البيانات، من خلال التخزين على السحابة، دوراً هاماً بالنسبة إلى الناس الواقعين في صراع. فالبيانات الشخصية الواقعة خارج العالم المادي ستكون أكثر أماناً بما أنه سيتعذر الوصول إليها. واندلاع العنف يفاجئ الجميع أحياناً، لكن في الحالات التي يكون فيها الوضع الأمني في تقهقرٍ واضح، سيفكر الأفراد باحتمال اضطرارهم إلى الهرب أو الانتقال، وسيتحضرون لذلك. وسيكون بوسعهم أيضاً دعم ادعاءاتهم بملكية بيوتهم وعقاراتهم وأعمالهم، حتى حين يكونون في المنفى أو لاجئين، عبر الاحتفاظ بأدلةٍ بصرية واستخدام أدوات مثل خرائط غوغل ونظام جي.بـي.أس لتحديد المكان. وسيكون بإمكانهم نقل وثائق ملكية الأراضي وغيرها من الوثائق العقارية إلى السحابة. وحين يوضع شيءٌ موضع الشك، ستساعد المنصات الرقمية في التحكيم. ويمكن للمدنيين الذين يدركهم النـزاع ويضطرهم للهرب أن يلتقطوا صوراً لجميع مقتنياتهم، وأن ينشئوا نموذجاً لمنـزلهم في الفضاء الافتراضي حيث يتمكنون عند عودتهم من معرفة ما هو مفقود لديهم بدقة. ومن الوارد جداً أن يتمكنوا من استخدام منصة شبكات اجتماعية للعثور على المواد المسروقة (بعد أن يكونوا قد أثبتوا رقمياً أنها تعود إليهم).

أتمتة الحروب

عندما يتصاعد نـزاع ما ويتحول إلى حرب مسلحة في المستقبل، سيجد المشاركون فيه أن ساحة المعركة قد باتت مختلفة تماماً عما كانت عليه في الماضي. ولن يغير فتح الجبهة الافتراضية للحرب حقيقة أنه مهما تطورت الأسلحة والجنود، ومهما بلغت أتمتتها، فسيكون عليها العمل في العالم الفيزيائي، ولن تستغني عن الدور الأساسي للتوجيه واتخاذ القرار البشريين. أما الجيوش التي لا تأخذ هذه الظاهرة مزدوجة العوالم (ومسؤولياتها في كل من العالمين) في الحسبان، فستجد أن التقانة الجديدة التي تجعلها ماكينات قتل أكثر فعالية تجلب عليها الكراهية أيضاً والتشهير؛ مما يجعل مشكلة كسب العقول والقلوب أصعب بكثير.

تمثل الأتمتة الحديثة للحروب، عبر التطورات التي شهدها مجال الروبوتات والذكاء الصنعي والطائرات من دون طيار، أهم تحول في القتال البشري منذ اختراع البندقية. فنحن أمام ما يصفه العلماء - كما ينوه الباحث العسكري بيتر سنغر في روايته المتقنة عن هذه النـزعة **مبرمج من أجل الحرب: ثورة الروبوتات وصراعها في القرن الحادي والعشرين** - ، وهي "حالة تصبح فيها

الأشياء مختلفة اختلافاً جذرياً، وتنهار فيها القواعد القديمة، حيث نصبح جاهلين بكل شيء عملياً". وكما يحدث كثيراً في أثناء التحولات التي تطرأ على الأطر النظرية عبر التاريخ (نظرية الجراثيم واختراع الطابعة ونظرية آينشتاين النسبية)، يكاد يكون مستحيلاً توقع - وبأي قدر مقبول من الدقة - كيفية تغيير هذا التحول النهائي إلى حرب مؤتمتة بالكامل مسار المجتمع البشري. ولا يبقى أمامنا سوى أن ننظر إلى الإشارات التي نراها اليوم، وأن نتخيل ما يجول بخاطر المقاتلين على الجبهات الأمامية، وأن نخمن قدر استطاعتنا.

ليس دمج تقانة المعلومات في آليات الحروب توجهاً جديداً. فقد تم إنشاء داربا؛ الجناح البحثي والتطويري للبنتاغون عام 1958 رداً على إطلاق القمر الصناعي سبوتنيك*. ونظراً إلى إصرار الحكومة على ألا تسمح بأخذها على حين غرة مرة أخرى، كانت مهمة داربا حرفياً "الحفاظ على التفوق التقاني للجيش الأمريكي، ومنع المفاجآت التقانية من إلحاق الأذى بالأمن القومي". بعد ذلك، أصبحت الولايات المتحدة رائدة العالم في مجال التقانة العسكرية المتقدمة وكل ما يتصل بها؛ بدءاً من القنابل الذكية، ووصولاً إلى الطائرات من دون طيار، وروبوتات إزالة المواد المتفجرة التي تعطل القنابل. لكن الولايات المتحدة - كما سنناقش لاحقاً - قد لا تحافظ على تفوقها الحصري لوقت طويل.

من السهل تفهم حب العسكريين والحكومات للروبوتات وغيرها من النظم غير المأهولة في المعركة، فهي لا تعرف التعب ولا الخوف ولا العاطفة، كما تتمتع بقدرات تفوق قدرات البشر، وتنصاع للأوامر دائماً. وكما يشير سنغر، إن الروبوتات مؤهلة على نحو فريد للعب الأدوار التي يسميها الجيش
. وما من شيء يحد الميزات التكتيكية التي تقدمها الروبوتات سوى محدودية مصنعيها، حيث يمكنهم صناعة روبوتات مقاومة للطلقات النارية ومُحكَمة التسديد وقادرة على التعرف على الأهداف ونـزع أسلحتها، وعلى حمل حمولات مستحيلة ضمن ظروف قاسية من الحرارة أو البرودة أو التشويش. والروبوتات العسكرية أفضل في تحملها وأسرع في رد فعلها من أي جندي. وسيكون السياسيون أكثر استعداداً لإرسالها إلى أرض المعركة مقارنة بالقوى البشرية. ويوافق معظم الناس على أن إدخال الروبوتات في العمليات الميدانية، سواء أتمّت على الأرض أم في البحر أم في الجو، سيؤدي في النهاية إلى عدد أقل من القتلى، وعدد أقل من الوفيات بين المدنيين، وقدر أقل من الأضرار المرافقة.

ثمة منذ اليوم أشكال كثيرة من الروبوتات المستخدمة في العمليات العسكرية الأمريكية، فقبل أكثر من عقد من الزمن، عام 2002، استحدثت شركة آي.روبوت - الشركة التي اخترعت مكنسة رومبا الكهربائية الروبوتية - روبوتاً أرضياً يدعى باك.بوت، وهو عبارة عن آلة بوزن 42 باوند (قرابة 20 كلغ) لها جنازير كجنازير الدبابة، ومزودة بكاميرات، وتعمل بدرجة معينة من الاستقلالية. ويمكن للوحدات العسكرية تجهيزها حيث تكتشف الألغام، وتستشعر وجود الأسلحة الكيميائية أو البيولوجية، وتتحقق من وجود أجهزة تفجير محسّنة على جوانب الطرقات أو في أي مكان آخر.

يصنّع مصنع روبوتات آخر، هو كوستر ميلر، منافساً لباك.بوت يدعى تالون، بالإضافة إلى روبوت مسلح آخر هو الأول من نوعه في دخول ميدان المعارك، ويسمى "نظام مراقبة الأسلحة الخاصة واستطلاعها واكتشافها"، أو سورد اختصاراً*. تأتي بعد ذلك الطائرات من دون طيار. فإضافة إلى طائرات بريديتر المعروفة اليوم، يشغل الجيش الأمريكي نسخاً أصغر منها (كطائرة رافن التي تطلق من اليد وتستخدم للمراقبة)، وأخرى أكبر حجماً (مثل ريبر التي تطير على ارتفاعات أعلى، وتصل إلى سرعات أكبر، وتحمل حمولة أسلحة أثقل من بريديتر). وقد ورد في تقرير داخلي من الكونغرس وصل إلى مدونة دنجر روم التابعة لمجلة "ويرد" عام 2012 أن هذه الطائرات تشكل اليوم 31 بالمئة من مجموع الطائرات العسكرية بعد أن كانت تشكل 5 بالمئة فقط عام 2005.

تحدثنا إلى عدد من الجنود السابقين والحاليين في القوات الخاصة لاستطلاع آرائهم حول أثر تقدم التقانات الروبوتية على العمليات القتالية خلال العقود القادمة، فتحدث هاري وينغو الذي يعمل اليوم لدى غوغل وكان أحد أفراد وحدة العمليات الخاصة الأمريكية، عن فائدة استخدام الحواسب بدلاً من البشر في المراقبة، وعن فائدة دفع الروبوتات في مقدمة القوات خلال التقدم عبر حقل نار أو عند إخلاء بناء. ففي العقد القادم - يقول - سيوكَلُ المزيدُ من

- أي العمليات التي تشتمل على إطلاق النار - إلى الروبوتات؛ بما فيها تلك الأعمال الشبيهة بالتنظيف، والتي تتطلب التعرف على الأهداف في أجزاء من الثانية. وسيبدأ الأمر بأن تعمل الروبوتات كمساعد آلي، بمعنى أن جندياً ما سيقوم بتوجيه الآلة من مكان بعيد. لكنها في النهاية - كما يعتقد وينغو - "ستتعرف بنفسها على الأهداف وتشتبك معها". ومنذ عام 2007، يقوم الجيش الأمريكي بتطوير روبوتات سورد المسلحة القادرة على التعرف على الأهداف البشرية وإطلاق النار عليها بشكل شبه مستقل، ولو أنه يعتقد أنه لم يتم استخدامها حتى الآن في سياق قاتل.

لن يترك الجنود للصفوف الخلفية بشكل كامل، إذ لن تتم أتمتة جميع الوظائف البشرية. فما من روبوتات تعمل اليوم بشكل مستقل تماماً (أي من دون أي توجيه من البشر). وكما سنناقش لاحقاً، ثمة جوانب هامة من العملية القتالية، كاتخاذ القرارات، ستعجز عنها الروبوتات لسنوات طويلة قادمة. ولاستيعاب التحسينات التي ستدخلها التقانة مباشرة على قدرات الجنود البشر، سألنا أحد أفراد وحدة العمليات الخاصة غير العامل حالياً، والذي كان بالمصادفة قد شارك في الهجوم على معقل أسامة بن لادن في أيار عام 2011، عما يتوقعه بشأن الوحدات المقاتلة في المستقبل. فأخبرنا أولاً أنه يتخيل وحدات مزودة بأجهزة لوحية آمنة في غاية التطور تسمح للجنود بالوصول إلى مدخلات فيديو حية من طائرات غير مأهولة، وتحميل تحليلات استخباراتية ذات صلة، والبقاء على اطلاع على مواقع القوات الصديقة وتحركاتها. وستحمل هذه الأجهزة خرائط حية فريدة يتم تحميلها بما يكفي من البيانات حول البيئة المحيطة؛ كالأهمية التاريخية لشارع ما أو مبنى، أو مالكي كل منـزل، وستقوم طائرة غير مأهولة بتصوير التحركات الحرارية تحت - الحمراء

الداخلية من الأعلى، وسترشد الجنود بشكل أوضح إلى ما ينبغي لهم استهدافه أو تجنبه.

ثانياً، ستتغير الألبسة والدروع التي يحملها الجنود. فالتقانات التماسية (التي تعتمد على الحس واللمس) ستتوصل إلى بذلات تسمح للجنود بالتواصل عبر النبضات، وبإرسال الإشارات إلى بعضهم؛ حيث تولد قرصة خفيفة أو رجة في جزء معين من الجسم (فقد تشير قرصة على بطن الساق اليمنى على سبيل المثال إلى أن حوامة على وشك الدخول). وستكون للخوذ رؤية أفضل، وستدمج فيها إمكانيات الاتصالات التي تسمح للقادة برؤية ما يراه جنودهم

بتوجيه الأوامر لجنودهم عن بعد من حيث يتواجدون في القاعدة. وسيسمح التمويه للجنود بتغيير لون بذلاتهم أو نسيجها البصري أو نقوشها أو رائحتها. بل قد تصبح البذلات قادرة على إصدار أصوات تطغى على الضجيج الذي يريد الجنود إخفاءه؛ كإصدار أصوات من الطبيعة تحول دون سماع أصوات وقع أقدام الجنود على سبيل المثال. وسيتم دمج مصادر طاقة خفيفة وطويلة الخدمة أيضاً؛ حيث لا تتوقف أي من الأجهزة أو التقانات الملبوسة عن العمل في اللحظات الحرجة نتيجة الحرارة أو البلل أو البعد عن مكان الشحن. وستتاح للجنود إمكانية إضافية، وهي تدمير جميع هذه التقانات عن بعد؛ حيث لا تتسرب أية أسرار استخباراتية ذات قيمة في حالات الأسر أو السرقة.

ستغطي كل ذلك بالطبع طبقة جبارة من الأمن السايبري (أقوى مما قد يستخدمه أي مدني) تسمح بالنقل الفوري للبيانات ضمن غلاف حماية إلكتروني. فمن دون الأمن، لن تستحق أي من الميزات السابقة التكاليف التي لا يستهان بها والتي يتطلبها تطويرها ونشرها. إلا أن إجراءات التعاقد في الجيش ستكبح الكثير من هذه التطورات. فالمجمع العسكري في الولايات المتحدة يعمل على بعض المبادرات المذكورة آنفاً (وقد قادت داربا تطوير العديد من الروبوتات قيد العمل اليوم)، لكنه بطبيعته غير مؤهل للتعامل مع الإبداع. فحتى داربا التي تتمتع بتمويل جيد نسبياً، غالباً ما تكبّلها بنى التعاقد المتضخمة والموقع الذي تحتله ضمن بيروقراطية وزارة الدفاع. وتبقى ميزة الإبداع التي لطالما كانت سمة من سمات قطاع التقانة الأمريكي معزولة عن جيش البلاد بجدران عالية تقوم على نظام مناقصات فوضوي بيزنطي؛ الأمر الذي يمثل فرصة مهدورة. ومن دون إصلاحات تسمح للوكالات العسكرية وللمتعاقدين بالتصرف على نحو أشبه بالشركات الخاصة الصغيرة الناشئة (بما تتمتع به من سهولة المناورة وسرعة التنقل)، فإن الصناعة برمتها مهددة بالانكماش بدلاً من التطور في ظل التقشف المالي.

يدرك الجيش هذه المشكلة تمام الإدراك. فكما يخبرنا سنغر، "ثمة سؤال استراتيجي كبير مطروح عليهم: كيف لهم الخروج من هذه البنية المتصدعة؟". فالمشاريع الدفاعية الكبرى تذبل في مرحلة النمذجة الأولية متجاوزة ميزانيتها ومتأخرة عن مواعيد تسليمها، بينما تستوحى التقانات والمنتجات التجارية اليوم من السوق، وتُصنّع وتوزع فيها بالجملة بوقت قياسي. فنظام الضم التكتيكي الراديوي الذي كان يفترض به أن يكون شبكة الاتصالات الراديوية الجديدة الشبيهة بالإنترنت

لدى الجيش، اقتُرح عام 1997 وتم إيقافه في أيلول عام 2012، ليتم تحويل وظائفه إلى الجيش تحت ما يسمى اليوم . وفي وقت إغلاقه كعملية مستقلة كان قد كلّف مليارات الدولارات من دون أن يكون قد نشر بشكل كامل في ميدان المعركة بعد، "لقد باتوا ببساطة عاجزين عن تمويل مثل هذه العملية"، يقول سنغر.

ثمة مخرج أمام الجيش ومتعاقديه، وهو استخدام منتجات تجارية جاهزة، أي شراء تقانات وأجهزة تجارية متوفرة بدلاً من تطويرها داخلياً. إلا أن دمج هذه المنتجات الخارجية لن يكون عملية سهلة، فمجرد تحقيق المتطلبات العسكرية (من متانة وفائدة وأمن) قد يتسبب بتأخيرات مدمرة. ووفقاً لسنغر، أدت البيروقراطية وانعدام الكفاءة في نظام التعاقد العسكري إلى مستوى غير مسبوق من الابتكار الميداني في اجتراح حلول وظيفية مواربة، كان من بينها شراء نظم لتلبية الحاجات السريعة خارج إجراءات المناقصات العادية لدى البنتاغون. وهي الطريقة التي تم بها دفع مركبات مراب (المضادة للألغام والمقاومة للكمائن) إلى الجبهة بعد أن بدأت كارثة أجهزة التفجير المحسنة في العراق. وغالباً ما تعتمد القوات تقانات تجارية تتولى نشرها بنفسها.

لقد أدرك القادة العسكريون أنفسهم المنافع التي تعد بها مثل هذه الابتكارية. "لقد كانت متطلبات ميدان القتال في العراق وأفغانستان هي التي تقود الجيش بطريقة ما" - يوضح سنغر - ففي أفغانستان، كان طيارو مروحيات البحرية الهجومية يربطون أجهزة آي.باد على ركبهم في أثناء التحليق، ويستخدمون نظام الخرائط فيها بدلاً من النظام المدمج في طائراتهم*، وأضاف أنه مع زوال الضغط الذي يفرض استعار ميدان القتال، يخشى القادة العسكريون أن تتلاشى هذه الحلول الالتفافية المبتكرة. ويبقى أن نرى ما إذا كان الإبداع سيفرض تغييراً في نظام التعاقد الإشكالي.

لطالما كانت الفتوحات التقانية تمنح الولايات المتحدة ميزات استراتيجية كبيرة في الماضي. فعلى مدى سنوات طويلة مرت على تطوير الصواريخ المقودة بالليزر لأول مرة، لم يكن لأي بلد آخر ما يضاهي قدرة الولايات المتحدة على الفتك من مسافات بعيدة. لكن الميزات التقانية تنـزع إلى التوزع عبر الوقت مع انتشار التقانات أو تسربها أو التوصل إليها عبر الهندسة العكسية، وليست الأسلحة المتطورة استثناء من ذلك. فسوق الطائرات غير المأهولة أصبحت سوقاً دولية منذ اليوم. حيث تسير إسرائيل في مقدمة الركب منذ سنوات، بينما تعمل الصين على ترويج طائراتها غير المأهولة وبيعها بلا هوادة. كما كشفت إيران عن أول مدمرة غير مأهولة محلية الصنع عام 2010. بل وانضمت فنـزويلا إلى القافلة بالاستفادة من تحالفها العسكري مع إيران، حيث شرعت ببرنامج طائرات غير مأهولة يشرف عليه مهندسو صواريخ إيرانيون. وعندما طلب من الرئيس الفنـزويلي هوغو شافيز أن يؤكد التقارير الواردة حول البرنامج قال: "بالطبع نقوم بذلك، ولنا الحق فيه، فنحن بلد حر مستقل". ستصبح الطائرات غير المأهولة أصغر حجماً وأرخص وأكثر فعالية مع مرور الوقت. وكما يحدث مع معظم التقانات، ما إن يتم توزيع المنتج في بيئته

(سواء أكان طائرة غير مأهولة أم تطبيقاً مكتبياً)، حتى تستحيل إعادته إلى العلبة.

سألنا ريجينا دوغان، المديرة السابقة في داربا، عن أسلوب تعاطي الولايات المتحدة مع المستوى العالي من المسؤولية الذي يتطلبه بناء مثل هذه الأشياء؛ علماً أن التبعات الأخيرة خارجة عن سيطرتها، فقالت: "غالباً ما تتسبب التقدمات التقانية، وخصوصاً الكبيرة منها، بتوتر الناس، ولدينا أمثلة جيدة وسيئة لتطوير نظام عمل اجتماعي وأخلاقي وقانوني يساير هذا النوع من التطورات التقانية". وتشير دوغان إلى المخاوف الأولية التي عبّر عنها الناس حيال الحمض الريبـي النووي للبشر، حين تم الإعلان عن هذا الفتح العلمي: فإذا أمكن تحديد قابليتك الفطرية للإصابة بمرض باركنسون، فكيف سيؤثر ذلك على طريقة تعامل أصحاب العمل وشركات التأمين معك؟ "لكن ما حدث فعلياً هو أنه تم إدراك أن الحل لا يكمن في تجنب التقدم الذي سمح لك برؤية قابليتك الفطرية"، توضح دوغان، "بل علينا أن ننشئ حمايات قانونية تضمن عدم حجب الرعاية الصحية عن الناس لأن لديهم استعدادات فطرية جينية". فلا بد من أن ترافق التقدمات التقانية الحمايات التي ستتطلبها بالنهاية لتحقيق التوازن الصحيح.

تصف دوغان الدور الذي تلعبه وكالتها السابقة بلهجة قاسية فتقول: "لا يمكنك أن تتولى مهمة مثل الاختراع ومنع التفوق الاستراتيجي إذا لم تكن مستعداً للقيام بأشياء تجعل الناس في البداية غير مرتاحين". فالواجب في الحقيقة هو أن تقوم بهذا العمل بمسؤولية. وهو ما سيتطلب قبل كل شي مساهمة الناس ومساعدتهم، "فالوكالة لا تستطيع القيام بذلك بنفسها، ولا بد من إشراك الفروع الحكومية والأطراف الأخرى في حوار يتناول هذه الأشياء".

من المريح أن يسمع المرء بمدى الجدية التي تتناول بها داربا مسؤوليتها حيال هذه التقانات الجديدة. لكن المشكلة تبقى بالطبع في عدم إبداء جميع الحكومات هذا القدر من التأني والحذر. فانتشار الطائرات غير المأهولة يمثل تحدياً مقلقاً على نحو خاص نظراً للميزات التي تمنحها حتى لأصغر الجيوش. وليست كل حكومة، أو كل جيش في العالم قادراً على تأمين البنية التحتية التقنية ورأس المال البشري اللازمين لدعم أسطول من المركبات غير المأهولة. فالحكومات الغنية هي وحدها التي ستجد سهولة في شراء مثل هذه الميزات سواء أفعلت ذلك علناً أم بطريقة أخرى. وستصبح حيازة الروبوتات العسكرية (وخصوصاً المركبات الجوية غير المأهولة) امتيازاً استراتيجياً لأي بلد. وستسعى بعض البلدان لاقتنائها لتحقيق التفوق، بينما ستسعى بلدان أخرى لاقتنائها لمجرد الحفاظ على سيادتها.

تحت سقف هذه المنافسة على مستوى الدول، سيكون هناك سباق محموم من قبل المدنيين وغيرهم من الفاعلين غير الحكوميين للحصول على الطائرات غير المأهولة والروبوتات أو بنائها لأهدافهم الخاصة. ويذكرنا سنغر بأن "الفاعلين غير الحكوميين، سواء أكانوا من الشركات - كالمجموعات الإعلامية وشركات رش المحاصيل الزراعية - أم من القوى التنفيذية أو من المجرمين والإرهابيين، يستخدمون جميعاً الطائرات غير المأهولة اليوم". وقد كشفت الشركة العسكرية الخاصة المثيرة للجدل بلاك ووتر، والتي أصبحت تسمى أكاديمي أل.أل.سي، عن

خدمتها الخاصة: "طائرات غير مأهولة متاحة للإيجار لأهداف المراقبة والاستطلاع"، عام 2007. وفي عام 2009 تم التعاقد معها لتحميل طائرات السي.آي.أيه غير المأهولة بالقنابل.

يجري تطوير الطائرات غير المأهولة واستخدامها على نطاق واسع بشكل خاص خارج سياق الاستخدامات العسكرية. إذ تستخدم بعض شركات العقارات على سبيل المثال الطائرات غير المأهولة الخاصة اليوم لالتقاط صور جوية لممتلكاتها الشاسعة. وتمتلك العديد من الجامعات طائراتها غير المأهولة الخاصة لأهداف بحثية. وقد افتتحت جامعة ولاية كنساس درجة في اختصاص الطيران غير المأهول. وفي عام 2012 سمعنا عن خدمة تاكو كوبتر، وهي خدمة تسمح لأي شخص يرغب في تناول شطيرة تاكو بطلبها عبر الهاتف الذكي وإدخال عنوانه ليستلم شطائره بواسطة طائرة غير مأهولة. وقد اكتشفنا في ما بعد أنها كانت مجرد خدعة، لكنها ممكنة تقنيًّا وغير مبالغ فيها.

كما ذكرنا سابقاً، سيكون هناك طلب خاص في سوق الأسلحة العالمية وفي الأسواق السوداء على الطائرات غير المأهولة الخفيفة والرخيصة التي تمت هندستها لأغراض قتالية. والطائرات والسيارات والقوارب النموذجية المقودة عن بعد، والقادرة على تولي مهام المراقبة واعتراض الأهداف المعادية وحمل القنابل وتفجيرها، ستفرض تحديات جدية على الجنود في مناطق الحرب، إذ ستضيف بعداً جديداً كاملاً على العمليات القتالية. وإذا وصلت النسخة المدنية من الطائرات غير المأهولة المسلحة إلى مستوى كاف من التطور، فقد نشهد قريباً طائرات غير مأهولة عسكرية ومدنية تلتقي في ميدان المعركة؛ ربما في المكسيك حيث يمتلك تجار المخدرات الرغبة والموارد اللازمة للحصول على مثل هذه الأسلحة.

ستسعى الحكومات إلى تقييد الوصول إلى التقانات الأساسية التي تسمح بالإنتاج الجملي للطائرات غير المأهولة من قبل العموم، لكن تنظيم انتشار هذه الطائرات المبتذلة وبيعها سيكون في غاية الصعوبة. إذ لن يكون من الواقعي ببساطة منعها بالكامل. وحتى إن المحاولات المتواضعة لضبط الاستخدام المدني لها في البلدان المسالمة لن تحقق سوى نجاح محدود. فإذا فرضت الحكومة الأمريكية على الناس مثلاً تسجيل طائراتهم غير المأهولة الصغيرة، وحددت الأجواء التي يمكن لهذه الطائرات التحليق فيها (بعيداً عن المطارات والأهداف الهامة على سبيل المثال)، ومنعت نقلها عبر حدود الولايات، فليس من الصعب تخيل أفراد يدفعهم إصرارهم إلى إيجاد طرق للالتفاف على هذه التشريعات بتعديل أجهزتهم وجعلها مغفلة الهوية، أو بتزويدها بنوع من القدرة على التخفي. إلا أننا سنشهد أيضاً إبرام اتفاقيات دولية تنظم انتشار هذه التقانات؛ ربما عبر منع بيع طائرات ذات أحجام كبيرة خارج القنوات الحكومية الرسمية. بل إن الدول الأكثر قدرة على نشر الطائرات غير المأهولة قد تعتمد بالفعل نسخة معاصرة من محادثات الحد من انتشار الأسلحة الاستراتيجية التي كانت الغاية منها تقليل عدد الأسلحة الأمريكية والسوفييتية خلال الحرب الباردة.

سيكون على الدول أن تعمل بجد للحفاظ على أمن شواطئها وحدودها في مواجهة التهديد المتنامي للطائرات غير المأهولة المعادية والمصممة بطريقة تصعّب على المراقبين اكتشافها. ومع توفر إمكانيات الملاحة المستقلة، ستصبح الطائرات غير المأهولة بمثابة صواريخ موجَّهة مصغرة؛ ما إن يتم إطلاقها حتى يتعذر إيقافها بالتشويش عليها. وقد تكون الطائرات المعادية غير المأهولة التي تستخدم لأهداف المراقبة مقبولة أكثر من تلك التي تحمل صواريخ على متنها. لكن كلا النوعين سيعتبر تهديداً بما أنه لن يكون من السهل التمييز بينهما. وربما لن تكون القوة أفضل طريقة لاستهداف طائرة معادية غير مأهولة، بل الأفضل استهدافها إلكترونياً عبر اختراق الدفاعات الأمنية السايبرية للمركبة. وبذلك تصبح الحرب - على حد تعبير سنغر - ، أي صراعاً على تجنيد هذه الآلات وإقناعها بالقيام بأشياء تختلف عن مهمتها. ففي أواخر عام 2011 عرضت إيران بفخر طائرة أمريكية غير مأهولة من طراز آر.كيو - 170 سنتينيل أنـزلت سليمة مدعية أنه تم الاستيلاء عليها عبر اختراق دفاعاتها بعد اكتشافها في الأجواء الإيرانية (وكل ما قالته الولايات المتحدة من طرفها هو أن المركبة قد ضاعت). وقد أخبر مهندس إيراني لم يذكر اسمه مجلة كريستيان سينس مونيتور أنه تمكن مع زملاء له من جعل الطائرة "تحط بنفسها في المكان الذي اخترناه من دون أن نضطر إلى فك إشارات التحكم عن بعد والاتصالات" من مركز التحكم الأمريكي بفضل ثغرة معروفة في نظام ملاحة جي.بـي.أس في الطائرة. وتقنية غرس إحداثيات جديدة، والتي تعرف بالتدليس، وإن كانت غير مستحيلة، تبقى صعبة للغاية (كان على الإيرانيين تجاوز التشفير العسكري للوصول إلى نظام جي.بـي.أس، ثم تدليس الإشارات والتشويش على قنوات الاتصال).

تُجترح حلول دبلوماسية تشتمل على معاهدات حسن نية بين الدول تتعهد فيها بعدم إرسال طائرات غير مأهولة للمراقبة في أجواء بعضها بعضاً، أو اتفاقيات ضمنية تعتبر الطائرات غير المأهولة والمستخدمة لأغراض المراقبة اعتداءً مقبولاً. من الصعب توقع ما سيحدث، فقد تفرض شروط على المستوى الدولي تنص على أن تكون طائرات المراقبة سهلة التمييز عن الطائرات القاذفة. وقد تتعاون بعض الدول لتشكيل نوع من "درع الطائرات غير المأهولة" في ما لا يختلف كثيراً عن التحالف النووي أيام الحرب الباردة؛ لنشهد بذلك أول منطقة حظر جوي للطائرات غير المأهولة في العالم. وإذا كان بلد صغير فقير عاجزاً عن بناء طائراته القاذفة غير المأهولة الخاصة أو شرائها، ويخشى التعرض لهجوم جوي من جار عدواني، فقد يسعى إلى التحالف مع قوة عظمى لضمان حد معين من الحماية. إلا أنه لا يبدو من الوارد أن تبقى الدول التي لا تمتلك طائرات غير مأهولة محرومة منها لوقت طويل، فطائرة سنتينيل للتجسس التي استولى عليها الإيرانيون لا تتجاوز كلفة تصنيعها 6 ملايين دولار.

سيزيد انتشار الروبوتات والطائرات غير المأهولة عدد النـزاعات في أنحاء العالم (فالدول التي ستحوزها، ستكون متحمسة لتجريب هذه الأدوات الجديدة)، لكنه سيخفف من احتمال اندلاع حرب شاملة. وثمة عدة أسباب لذلك، منها أن هذه

الظاهرة لا تزال جديدة جداً من ناحية، والاتفاقيات الدولية التي تتناول الأسلحة والحروب (كمعاهدة حظر انتشار الأسلحة النووية، ومعاهدة حظر انتشار الصواريخ البالستية، واتفاقية الأسلحة الكيماوية، وغيرها) لم تواكب بعد عصر الطائرات غير المأهولة من ناحية أخرى. فثمة حدود يجب رسمها، وأطر قانونية يجب تطويرها، وسياسيون يجب أن يتعلموا كيف يستخدمون هذه الأدوات بمسؤولية وعلى مستوى استراتيجي. وثمة اعتبارات أخلاقية خطيرة سيتم تناولها في المناقشات العامة (كتلك الجارية اليوم في الولايات المتحدة). وستدفع جميع هذه النقاط الدول إلى إبداء الحذر خلال السنوات الأولى لانتشار الطائرات غير المأهولة.

علينا أيضاً التفكير في احتمال ظهور مشكلة الطائرات غير المأهولة السائبة؛ على غرار ما نشهده اليوم في مجال الأسلحة النووية. ففي بلد مثل باكستان على سبيل المثال، ثمة مخاوف جدية من عجز الدولة عن حراسة مخزونها النووي (الذي يقدر بمئة رأس نووي) من السرقة. ومع تطوير الدول أساطيل كبيرة من الطائرات غير المأهولة، ستكون هناك خطورة أكبر تتمثل في وقوع إحداها في الأيدي الخطأ، واستخدامها ضد سفارة أجنبية أو قاعدة عسكرية أو مركز ثقافي. فتخيل أحداث الحادي عشر من أيلول في المستقبل ترتكب ليس من قبل مختطفي طائرات تجارية، بل بواسطة طائرات غير مأهولة خرجت من يد الدولة. فهذه المخاوف كفيلة بالتحفيز على إبرام معاهدات مستقبلية تركز على وضع شروط لحماية الطائرات غير المأهولة وحراستها.

سيكون على الدول أن تقرر - بشكل فردي أو جماعي - القواعد الناظمة للطائرات غير المأهولة، وما إذا كانت ستفرض عليها القواعد الناظمة لملاحة الطائرات العادية نفسها في ما يتعلق بانتهاك الأجواء ذات السيادة. وسيتكفل الخوف المتبادل للدول بمنع حدوث تصعيد سريع يؤدي إلى حرب بالطائرات غير المأهولة. فحتى عندما تم الكشف عن اختراق طائرة سنتينيل الأمريكية للأجواء الإيرانية، اقتصر رد فعل طهران على التفاخر والاستعراض من دون التفكير في الانتقام.

ستفضل الجماهير تخفيف حدة معارك الطائرات غير المأهولة، مما سيتكفل بتلافي نشوب حرب شاملة في المستقبل. وقد سبق لنا أن شهدنا بضع سنوات من الدورات الإخبارية المتعلقة بالطائرات غير المأهولة في أمريكا، والتي يمكننا استقاء الدروس منها. فقبل بضعة شهور على الانتخابات الرئاسية عام 2012 تسببت تسريبات حكومية بظهور مقالات مفصلة عن العمليات السرية للطائرات غير المأهولة للرئيس أوباما. وإذا أردنا أن نحكم من خلال ردود الفعل على ضربات الطائرات غير المأهولة، سواء أكانت في ساحات القتال الرسمية أم غير الرسمية كما في الصومال واليمن وباكستان، فإن المهام القاتلة التي تنفذها طائرات غير مأهولة تحظى بقدر أكبر من القبول لدى الجمهور الأمريكي مقارنة بتلك التي تنفذها القوات. حيث تثير عدداً أقل من الأسئلة، وقدراً أقل من الغضب الشعبـي. بل إن بعض المدافعين عن تخفيف التواجد الأمريكي ما وراء البحار، عبروا عن دعمهم للتوسع في برنامج الطائرات غير المأهولة كوسيلة شرعية لتحقيق غايتهم.

لا يمكننا بعد استيعاب التبعات (السياسية والثقافية والنفسية) التي ستترتب على قدرتنا الجديدة على استغلال المسافة الفيزيائية والعاطفية وإلغاء الصفة البشرية عن الحرب إلى هذه الدرجة بالفعل. فالحرب عن بعد تجري اليوم أكثر من أي وقت مضى في التاريخ. وهي لن تزداد إلا انتشاراً، وستصبح سمة بارزة من سمات الصراعات. وإذا كانت الحرب عن بعد تعني تاريخياً استخدام أسلحة محملة على صواريخ، فسيزداد في المستقبل شيوع وتقبل فصل الفاعل عن ميدان المعركة. وإذا نظرنا إلى التوجهات السائدة، يمكننا افتراض أن هذه التغيرات ستؤدي - من بين نتائج أخرى - إلى قدر أقل من المشاركة الشعبية على المستويين العاطفي والسياسي. فالخسائر البشرية على الطرف الآخر، في نهاية المطاف، قلما تكون عاملاً محركاً للسياسة الخارجية أو للرأي العام. وحين لا يُرى أن القوات الأمريكية عرضة للأذى، سيهبط مستوى الاهتمام الشعبـي هبوطاً ملحوظاً؛ مما يعني زيادة الصمت الشعبـي إزاء مسائل الأمن القومي. فعندما يكون الخطر الذي يلوح في الأفق على الجنود صغيراً، تتبدد المخاوف لدى الصقور كما لدى الحمائم. ومع توفر المزيد من الخيارات القتالية التي لا تثير الرأي العام، ستستطيع الحكومة تحقيق أهدافها الأمنية من دون أن تضطر إلى التفكير في إعلان الحرب أو في إرسال القوات؛ مما سيقلل احتمال نشوب حرب كاملة.

سيكون انخفاض الخسائر البشرية المتوقعة بين المدنيين، وانحسار الأضرار في الممتلكات، وتراجع احتمال تضرر البشر موضعَ ترحيب. لكن الانتقال إلى ميدان قتال مؤتمت بالكامل سيكشف عن ثغرات جديدة وسيفرض تحدياته. وسيكون أبرز هذه التحديات هو الحفاظ على الأمن السايبري للمعدات والأنظمة. إذ يجب أن يكون تدفق البيانات بين الأجهزة والروبوتات الأرضية والطائرات غير المأهولة من جهة، ومراكز قيادتها والتحكم بها التي يديرها البشر من جهة أخرى، سريعاً وآمناً لا تعيقه رداءة البنية التحتية؛ تماماً كما هي الاتصالات بين الوحدات المقاتلة وقواعدها. وهذا هو ما يدفع الجيوش لتشغيل شبكات اتصالاتها الخاصة بدلاً من الاعتماد على الشبكات المحلية. وإلى أن تُزوَّد الروبوتات في الميدان بذكاء صنعي مستقل سيبقى اعتراض اتصالاتها أو قطعها كفيلاً بتحويل هذه الآلات إلى عبء إضافي مكلف، بل قد يجعلها خطيرة أيضاً بما أن الاستيلاء على روبوت للعدو يعد بمثابة الوصول إلى تقانة ذات ملكية، ويفتح إمكانيات لا نهاية لها؛ خصوصاً إذا كان الروبوت سيئ التصميم. فهو لن يكشف عن معلومات حول البرمجيات وهندسة الطائرة غير المأهولة فقط، بل وعن بيانات أكثر حساسية كمواقع تموضع العدو التي تلتقط عبر الإحداثيات الرقمية (ومن الصعب في الوقت نفسه تخيل أن تحجم البلدان عن جعل طائرات غير مأهولة مفخخة وتقوم بهبوط اضطراري، أو تعرض نفسها للاختراق بعد ملئها بمعلومات مزيفة وبمكونات تقنية مضللة كجزء من حملة تضليل). ففي الحروب التي تشتمل على عناصر روبوتية، سيسعى الطرفان إلى شن هجمات سايبرية لمقاطعة نشاطات العدو، سواء أتمّ ذلك عبر التدليس (بانتحال هوية شبكية)، أو بتوظيف أجهزة استدراج تشوش على شبكات حساسات العدو وتؤثر على فعاليات شبكاته القتالية. وسيحاول المصنعون بناء آليات وقائية

تخفف من الضرر الناجم عن مثل هذه الهجمات، لكن سيكون من الصعب بناء أي شيء منيع تماماً من الناحية التقانية.

سيكون على الجيوش وعلى مطوري الروبوتات معالجة الأخطاء البسيطة أيضاً. فجميع الأنظمة الشبكية تعاني من الثغرات ونقاط الضعف، وغالباً ما تكون الطريقة الوحيدة للكشف عنها هي اللجوء إلى المخترقين وخبراء نظم الأمن المستقلين. فالشيفرات الحاسوبية اللازمة لتشغيل آلات بهذه القدرات هائلة الحجم (ملايين الملايين من أسطر الشيفرة البرمجية)، والأخطاء تحدث. وحتى عندما يكون المطورون مدركين لنقاط ضعف النظام، فإن معالجتها ليست بالأمر السهل. فالثغرة التي قال الإيرانيون إنهم استغلوها في هجومهم لإسقاط الطائرة الأمريكية غير المأهولة نقطة ضعف في نظام جي.بـي.أس يقال إن البنتاغون كان يعلم بها منذ الحملة على البوسنة في تسعينيات القرن العشرين. وفي عام 2008 اكتشفت القوات العسكرية الأمريكية للمرة الأولى حواسب محمولة تعود لمتمردين في العراق تحتوي على ملفات لإشارات فيديو تم اعتراضها، والتي استطاع العراقيون الوصول إليها بمجرد توجيه أطباقهم الفضائية اللاقطة؛ مستخدمين برمجيات رخيصة متاحة للتحميل تدعى سكاي غرابر، وتكلف 26 دولاراً، الهدف الأصلي منها هو مساعدة الناس على قرصنة الأفلام والموسيقى. فبيانات الاتصالات بين الطائرة غير المأهولة وقاعدة التحكم الأرضية لم تكن مشفرة على الإطلاق.

سيشهد المستقبل القريب أخطاء جديدة مع استمرار البشر في تطبيق هذه التقانات. ووضع النفس البشرية الهشة في مواقف قتالية متطرفة سيؤدي دائماً إلى حالات غير متوقعة؛ فقد يؤدي إلى اضطراب ما بعد الصدمة أو اكتئاب عاطفي حاد أو انهيار نفسي كامل. ولا بد من أخذ هذه الأخطاء في الحسبان طالما استمر البشر في خوض الحروب.

إلى أن تتمكن نظم الذكاء الصنعي من محاكاة قدرة الدماغ البشري، لن نشهد أية نظم غير مأهولة تحل محل الجنود البشر بالكامل؛ كأفراد أو كمتخذي قرارات. فحتى أكثر الآلات ذكاء قد ترتكب أخطاء فاضحة. ويشير بيتر سنغر إلى أنه خلال الحرب العالمية الأولى، عندما ظهرت الدبابة للمرة الأولى في ميدان المعركة بما تحمله من عتاد ودروع وجنازير، ساد اعتقاد بأنه لا يمكن إعطابها، إلى أن خرج أحدهم بفكرة الخندق المضاد للدبابات. وها هو وزير الدفاع الأفغاني السابق عبد الرحيم ورداك، الذي قابلناه في كابول قبيل إقالته، يضحك وهو يصف لنا كيف كان يستهدف الدبابات السوفييتية مع رفاقه المجاهدين في ثمانينيات القرن العشرين، وكيفية بنائهم أشراكاً مغطاة بأوراق الشجر، تشبه تلك التي كان الفيتكونغ يقيمونها للإيقاع بالجنود الأمريكيين قبل عقد من الزمن. يوازي ذلك في يومنا - كما يقول سنغر - أن "[تستخدم][تستخدم][تستخدم][تستخدم][تستخدم] الروبوتات الأرضية التي يستعملها جنودنا في العراق وأفغانستان تقانة مدهشة، لكن المتمردين سرعان ما سيدركون أن بإمكانهم الإيقاع بها بنصب أفخاخ النمور، وهي مجرد حفر عميقة تسقط فيها. بل إنهم ربما يتوصلون إلى زاوية الانحدار التي يفشل عندها الروبوت بالتسلق والخروج من الحفرة". فذكاء هذه الروبوتات متخصص، ومع اختبارها

ميدانياً سيتعرف مشغلوها ومطورها باستمرار على ظروف معادية ما كانوا ليتوقعوها؛ مما سيضطرهم إلى تطوير منتجاتهم. وستبقى المواجهات غير المتكافئة كهذه مصدراً للتحديات غير المتوقعة حتى بالنسبة إلى التقانات الأكثر تطوراً.

إلا أن الذكاء البشري لا ينحصر بمهارات حل المشكلات. فالبشر يتحلون بخصال قتالية (كإصدار الأحكام والتعاطف والثقة) يصعب تعريفها، ناهيك عن دمجها في روبوت. فما الذي سيضيع مع تولي الروبوتات على نحو مضطرد مسؤوليات البشر في ميدان المعركة؟ خلال محادثاتنا مع أفراد القوات الخاصة، أكد هؤلاء على الأهمية البالغة للثقة ولشعور الأخوة في تجاربهم الميدانية. فمنهم من تدربوا وقاتلوا معاً لسنوات، فتعرفوا على عادات بعضهم وتحركاتهم وطرق تفكيرهم بطريقة فطرية. وهم يقولون إن باستطاعتهم التواصل بمجرد نظرة. فهل ستستطيع الروبوتات ذات يوم أن تحاكي القدرة البشرية على قراءة الإيماءات غير المنطوقة؟

هل يستطيع الروبوت أن يكون شجاعاً؟ وهل يمكنه أن يضحي بلا أنانية؟ هي يمكن لروبوت مدرب على التعرف على الأهداف والاشتباك معها أن يتحلى ببعض الأخلاق وبضبط النفس؟ وهل سيتمكن أي روبوت من التمييز بين طفل ورجل صغير؟ وإذا قتل روبوت مدنياً بريئاً، فعلى من سيلقى اللوم؟ تخيل مواجهة بين روبوت أرضي مسلح وطفل في السادسة من عمره يحمل عبوة بخاخ ملون أرسلته ربما مجموعة متمردة. فسواء أتصرف الروبوت على نحو مستقل أم بتوجيه من البشر، سيكون بمقدوره إما إرداء الطفل الأعزل أو أن يتعطل حين يوجّه الطفل المادة الملونة إلى كاميراته ذات التقانة العالية ومكنوناته الاستشعارية مسبباً له العمى. فما الذي ستفعله إذا كنت مسؤولاً عن اتخاذ مثل هذا القرار، وكانت قيادة الروبوت في يدك؟ يسألنا سينغر. لا يمكننا محاكمة الروبوتات أو محاسبتها أو التحقيق معها. لذا، إن البشر سيحافظون على سيطرتهم على العمليات القتالية لسنوات طويلة قادمة، حتى مع ازدياد الروبوتات ذكاءً وتكاملاً مع القوات البشرية.

التدخلات الجديدة

إن دخولنا عصر النـزاعات الافتراضية والحروب المؤتمتة يعني أن الدول ذات الأجندات العدوانية ستجد بين يديها طيفاً واسعاً من الأدوات التي يمكنها استخدامها في المستقبل. كما أن تدخلات الفاعلين الآخرين (من مواطنين وشركات وحكومات) ستزداد تنوعاً بدورها.

أما بالنسبة إلى الدول، فسيبقى مجلس الأمن التابع للأمم المتحدة الهيئة الدولية الوحيدة التي تضم جميع الأمم، والقادرة في الوقت نفسه على إضفاء الشرعية على التدخلات العسكرية التي تقودها الدول. ومن غير الوارد أن يخرج المجتمع الدولي عن هذا الترتيب للقوى العظمى، الذي يعود لعام 1945، والذي شكّل حجر الأساس للأمم المتحدة؛ حتى إذا تعالت صرخات المواطنين المتمكنين الذين يطالبون دولهم بالتصرف. وسيستحيل تقريباً عقد انتدابات جديدة، أو الاتفاق على تدخلات جديدة، لأن أية تعديلات على ميثاق الأمم المتحدة ستتطلب موافقة 194

دولة عضواً.

لكن، ثمة مجالات ذات مستوى عالٍ من الحنكة السياسية، قد تكون أشكال جديدة من التدخل أكثر قابلية للاستمرار فيها، وسيأتي تنفيذها على شكل تحالفات أصغر. ففي الحالات الأكثر تطرفاً، سنشهد مجموعة من الدول التي تتعاون في ما بينها لتعطيل روبوتات عسكرية تعود لدولة ضالة على سبيل المثال. كما يمكننا تخيل ممارسة بعض الدول الأعضاء في الناتو ضغطاً من أجل إقامة انتدابات جديدة تسمح بالتدخل، وتخول الدول إرسال قوات محاربة إلى مناطق النـزاع لإقامة مناطق آمنة تقام فيها شبكات مستقلة غير مخترقة. وستصبح هذه فكرة شائعة في دوائر سياسات التدخل، فهي تمثل امتداداً طبيعياً لمبدأ الذي استخدمه مجلس الأمن لترخيص العمل العسكري (مع الضربات الجوية) في ليبيا عام 2011، والذي نفذه الناتو في ما بعد على هذا الأساس. ومن الوارد جداً أن نرى أعضاء في الناتو يساهمون بطائرات غير مأهولة لإقامة أول منطقة حظر جوي غير مأهولة في العالم فوق مناطق يسيطر عليها ثوار، من دون إرسال أية قوات ومن دون تعريضها للخطر.

بعيداً عن المؤسسات الرسمية كالناتو، سيجد الضغط من أجل التصرف متنفّساً له على شكل تحالفات سريعة يشارك فيها المواطنون والشركات. فهؤلاء لا يستطيعون حشد القوة العسكرية التي يتطلبها التدخل الميداني، لكنهم يستطيعون المساهمة عبر صيانة شبكات الاتصالات ذات الأهمية الحيوية في مناطق الصراع. وستتجسد التدخلات المستقبلية في إعادة وصل الإنترنت، أو مساعدة المناطق التي يسيطر عليها الثوار على إعداد شبكة مستقلة وآمنة. وفي حالات التلاعب بالاتصالات من قبل الدولة أو بدعم منها، سينسق اللاعبون الدوليون جهودهم للتدخل ولاستعادة الوصول الحر والمستمر؛ من دون انتظار موافقة الأمم المتحدة.

ليست الاتصالات بحدّ ذاتها هي الأساس (فقد يتوفر لدى المواطنين في مناطق الصراع مسبقاً شكل من أشكال الاتصالات)، بل ما يستطيع الناس فعله من خلال شبكة آمنة وسريعة. حيث سيتمكن الأطباء في المستشفيات الميدانية المؤقتة من التنسيق بسرعة على المستوى المحلي أو الدولي لتوزيع الإمدادات الطبية، وتنظيم الإنـزالات الجوية، وتوثيق المشاهدات. وسيتمكن المقاتلون المتمردون من التواصل بأمان بعيداً عن شبكة الاتصالات الحكومية ضمن نطاقات، وعلى منصات أكثر فائدة بكثير من الراديوهات. وسيتمكن المدنيون من التواصل مع أفراد عائلاتهم في الخارج عبر منصات كانت ستبقى محجوبة لولا ذلك، وعبر قنوات آمنة (تكون بشكل أساسي أدوات بروكسي وأدوات التفافية) لإرسال المال أو المعلومات إلى الخارج.

وقد تقوم تحالفات دولية بإرسال ما يكافئ وحدات القوات الخاصة لمساعدة الحركات الثورية على الانفصال عن الشبكات الحكومية وتأسيس شبكاتها الخاصة. وهي مبادرات يتم اتخاذها اليوم بالفعل، لكن على نحو مستقل. فقد أخبرتنا مجموعة من الوزراء الليبيين قصة عن أمريكي شجاع يدعى فريد وصل إلى معقل الثوار في بنغازي على متن قارب خشبـي، مسلحاً بمعدات اتصال ومصمماً على

مساعدة الثوار على بناء شبكة اتصالاتهم الخاصة. وكانت أول مهمة لفريد هي إزالة أجهزة التنصت العائدة إلى حقبة القذافي. لكن في المستقبل، ستصبح مثل هذه العمليات بمثابة عمليات قتالية؛ خصوصاً في الأماكن التي لا يمكن الوصول إليها عبر البحر.

سيتغير تركيب تحالفات التدخل أيضاً. فالدول ذات الجيوش الصغيرة والقطاعات التقانية القوية ستصبح في عداد أصحاب النفوذ الجدد. فبنغلادش اليوم هي البلد الأكثر إسهاماً بالقوات في مهام حفظ السلام الدولية. أما في المستقبل، فستكون البلدان ذات القطاعات التقانية القوية، والتي تشمل حالياً أستونيا والسويد وفنلندا والنرويج وتشيلي، هي التي تتسلم قيادة هذا النوع من المهام. وستؤمن التحالفات القائمة على الاتصالات ما يلزم من إرادة سياسية وأسلحة رقمية؛ كالاتصالات ذات عرض الحزمة العالي، والشبكات النقالة المستقلة المرتجلة، والأمن السايبري المحسن. وقد تساهم هذه الدول أيضاً بالتدخلات العسكرية، لكن باستخدام روبوتاتها وأساطيل المركبات غير المأهولة الخاصة بها. فبعض الدول، وخصوصاً الصغيرة منها، ستجد في بناء ترسانتها الخاصة من المركبات غير المأهولة وإرسالها مع القوات متعددة الجنسيات وسيلةً أرخص وأكثر قبولاً سياسياً مقارنة ببناء قوات بشرية ونشرها.

ستشارك في هذه التحالفات شركات التقانة والمنظمات غير الحكومية، وسيقدم كل منها شيئاً ما ذا قيمة خاصة؛ وهذا ما سيفعله الأفراد أيضاً. إذ ستبني الشركات برمجيات مفتوحة المصدر مخصصة لحاجات الشعب داخل البلد، وستقدّم تحديثات مجانية لجميع منتجاتها، بينما تقوم المنظمات غير الحكومية بالتنسيق مع شركات الاتصالات ببناء قواعد بيانات دقيقة لشعب معين واحتياجاته، وإعداد خرائط تبين الجيوب الأكثر اضطراباً وعزلة. وسيكون بإمكان المواطنين التطوع لاختبار الشبكة الجديدة وجميع هذه المنتجات، والمساعدة على العثور على الثغرات ونقاط الضعف، إضافة إلى تقديمهم كمستخدمين تغذية راجعة غاية في الأهمية.

مهما بلغ تطور التقانة لدينا، فإن الصراعات والحروب ستجد جذورها دوماً في العالم المادي الذي ستبقى فيه القرارات المتعلقة بنشر الآلات واتباع التكتيكات السايبرية منوطةً بالبشر بشكل أساسي. ومن شأن التقانة، بصفتها عامل مساواة، أن تحسن قدرات جميع أطراف النـزاع وتمكنهم من القيام بالمزيد. أي المزيد من التراسل، والمزيد من المحتوى من جميع الأطراف، والمزيد من استخدام الروبوتات والأسلحة السايبرية، وطيف أوسع من الأهداف الاستراتيجية التي يمكن ضربها. وثمة تحسينات واضحة؛ كإمكانية المحاسبة التي تفرضها ديمومة الأدلة. لكن التقانة ستعقّد النـزاع في النهاية، بقدر ما تخفض المخاطر التي ينطوي عليها إجمالاً.

سيجد مقاتلو المستقبل (من دول وثوار وجيوش) أن الحسابات الأخلاقية والتكتيكية والاستراتيجية الصارمة التي كانوا يستخدمونها في الصراعات المادية بات عليها أن تشمل أيضاً الجبهة الافتراضية التي ستؤثر على آلية اتخاذ القرار في

كثير من الأحيان. وسيؤدي ذلك إلى مزيد من التحركات من قبل المعتدين في الجبهة الافتراضية الأقل مخاطرة - كما شرحنا سابقاً - لما تقدمه من إمكانيات التمييز وتنفيذ الاجتياحات السايبرية الاستباقية التي يصعب تحديد مصدرها. وفي حالات أخرى، ستلعب الجبهة الافتراضية دور القوة الكابحة التي تدفع المعتدين إلى تقييم درجة عنفهم على الجبهة المادية. وكما سيتوضح لنا أكثر بعد خلال الصفحات القادمة، إنّ مجرد وجود جبهة افتراضية سيعبّد الطريق أمام استنباط خيارات التدخل الفعالة، والتي تخفض في الوقت نفسه من الحاجة إلى إرسال قوات وتعريضها للخطر بشكل عام. فقد يصبح من الممكن إقامة مناطق حظر جوي تخفرها طائرات غير مأهولة، وتنظيم مهام حفظ السلام الروبوتية خلال الصراع، لكن مثل هذه الخطوات تبقى محدودة. وعندما ينقضي النـزاع على أية حال، وتبدأ جهود إعادة الإعمار، تصبح فرص إعادة بناء البلاد بمساعدة التقانة غير محدودة.

الفصل السابع: مستقبل إعادة الإعمار

بات من الواضح تماماً اليوم كيف يمكن استخدام التقانة لقلب المجتمعات رأساً على عقب، بل ولتمزيقها. لكن، ماذا عن إعادة توحيدها؟ إن إعادة الإعمار بعد نـزاع أو كارثة طبيعية عملية طويلة ومجهدة، وليست شيئاً يمكن إنجازه عبر الاحتشادات الخاطفة أو حملات الفيديو الفيروسية. لكن، إذا كانت تقانات الاتصالات وحدها لا تكفي لإعادة إعمار المجتمعات المحطمة، فإنها قادرة على تحسين جميع الجهود السياسية والاقتصادية والأمنية وتسريعها. وستجد الأدوات التي نستخدمها للترفيه العَرَضي اليوم غاية جديدة لها في المستقبل في المجتمعات الخارجة من أزمة. إذ ستجد الشعوب المحتاجة مزيداً من المعلومات، ومزيداً من القوة بين يديها. وستصبح مشاريع إعادة الإعمار ابتكارية وأكثر شمولاً وفعالية مع الوقت، بعد أن تكون النماذج والطرائق القديمة قد حُدِّثت أو تم التخلي عنها. والتقانة لا تستطيع الحيلولة دون وقوع كارثة، أو إيقاف حرب أهلية، لكنها تستطيع جعل عملية إعادة التجميع أقل إيلاماً.

تماماً كما ستشهد الصراعات في المستقبل إضافة الجبهة الافتراضية، سيحدث الشيء نفسه مع مشاريع إعادة الإعمار. وستبقى لدينا الرافعات والجرافات التي ترمم الطرق وتعيد بناء الجسور وتبعث الحياة في الأبنية المهدمة، لكننا سنشهد أيضاً - على التوازي مع ذلك - تركيزاً مباشراً على وظائف أساسية كانت في الماضي غالباً ما تترك حتى نهاية العملية. فإعداد الاتصالات وتشغيلها على سبيل المثال سيمكن من إعادة بناء البنية التحتية المادية، والبنية التحتية الاقتصادية والحكومية في الوقت نفسه. سنوجز في ما يلي رؤيتنا للأسلوب الذي سيتبعه مخططو إعادة الإعمار في المستقبل في مجتمعات ما بعد الأزمة، وسنتطرق في نقاشنا إلى موجة من المشاركين الجدد الذين ستحفزهم إمكانيات الاتصالات الجديدة على المبادرة وعلى اقتراح أفكار جديدة لتبني سياسات مبتكرة تستطيع وضع المجتمعات على طريق أسرع نحو التعافي.

الاتصالات أولاً

تشكل إعادة الإعمار بالنسبة إلى المجتمعات الخارجة من كارثة، طبيعية أو من صنع البشر، مهمة مهولة. فمن إعادة فتح الطرق وترميم المباني، إلى إعادة وصل الشعب بالخدمات التي يحتاج إليها، تتطلب هذه التحديات موارد هائلة وأنواعاً مختلفة من الخبرات التقنية، إضافة إلى الصبر بالطبع. ومن شأن التقانة الحديثة أن تساعد في هذه العمليات مساعدة كبيرة إذا تم توظيفها بالطرق الصحيحة. ونحن نعتقد أن مشاريع إعادة الإعمار الناجحة في المستقبل ستعتمد بشكل كبير على تقانات الاتصالات وعلى شبكات الاتصالات السريعة.

سيكون هناك نموذج أولي لإعادة الإعمار يضم مجموعة مرنة ومبوبة من الممارسات القابلة للتكييف والنماذج التي يمكن تفصيلها بما يتناسب مع بيئات ما -

بعد - أزمية معينة. وتستخدم شركات التقانة مثل هذه النماذج الأولية ونماذج لترك مجال للتجربة والخطأ، بناءً على فلسفة تقول إن التغذية الراجعة في المراحل المبكرة من استخدام منتج غير كامل ستؤدي في النهاية إلى نتائج أفضل (ومن هنا القول المأثور المفضل لدى متعهدي التقانة: أخطئ مبكراً، أخطئ كثيراً). وسيستغرق تطوير أسلوب شبيه بالنمذجة الأولية في إطار مشاريع إعادة الإعمار بعض الوقت، لكنه في النهاية سيخدم المجتمعات المحتاجة بشكل أفضل.

وسيكون المكون الرئيس في النموذج الأولي لإعادة الإعمار (وما يميزه عن، لنقل، مشاريع إعادة الإعمار الأكثر تقليدية) هو عقلية ، أو ، وقد أصبح ترميم شبكات الاتصالات وتحديثها منذ اليوم بمثابة الإسمنت الجديد في مشاريع إعادة الإعمار الحديثة. وإذا نظرنا إلى الأمام، فإن الارتقاء بالمجتمعات المدمرة والوصول بها إلى بنية اتصالات تحتية سريعة وعلى أحدث طراز سيكون الأولوية الأولى لجميع المشاركين في عمليات إعادة الإعمار، وليس فقط لأن نجاح عملهم سيعتمد عليها. وهو تحول نشهده منذ العقد الماضي.

منذ بداية العقد الأول من القرن الحادي والعشرين، لم تعد عمليات إعادة الإعمار بعد النـزاعات تركز على إعادة إحياء الاتصالات بقدر ما تحاول إقامتها من جديد. إذ لم يكن هناك أي شكل من أشكال الشبكات النقالة في أفغانستان، وكذلك في العراق قبل تغير النظام؛ حيث كانت حكومة طالبان تعارض بعنف جميع أشكال تقانة المستهلك تقريباً (وإن كانت لديها شبكة جي.أس.أم، وهي نظام الاتصالات النقالة العالمي، والتي كانت محصورة بمسؤولي الحكومة). بينما كان صدام حسين يمنع الهواتف النقالة برمتها في دولته. وعندما سقطت هذه الأنظمة، وجدت الشعوب نفسها من دون بنى تحتية أو أجهزة حديثة عملياً، وكان المتصارعون في الصراعات التالية هم وحدهم الذين يمتلكون شكلاً ما من أشكال الاتصالات المحمولة (على شكل اتصالات راديوية عادةً).

عندما دخلت فرق إعادة الإعمار المدنية الأمريكية العراق عام 2003 وجدت نفسها في صحراء اتصالاتية. وانتهت المساعي الأولى لاستخدام الهواتف الفضائية إلى التخبط عندما اكتُشِف أن الهواتف لا تعمل إلا إذا كان كلا المستخدمَين يقفان في الخارج، وهي ميزة مزعجة بلا شك في منطقة حرب. وكحل عاجل، منحت سلطة الائتلاف المؤقتة شركة أم.تي.سي - فودافون، وهي شركة اتصالات إقليمية، عقداً لتركيب الأبراج الخلوية ولتقديم خدماتها في جنوب البلاد، بينما حصلت شركة اتصالات أخرى هي أم.سي.آي على موافقة على عملها في بغداد. ووفقاً لأحد كبار المسؤولين السابقين في السلطة كنا قد تحدثنا معه، وضعت الأبراج في جميع أنحاء البلاد بين ليلة وضحاها حرفياً. حيث تلقى المسؤولون وأفراد الأمم المتحدة آلاف الهواتف الخلوية ليوزعوها على اللاعبين السياسيين المحليين الهامين (الغريب أن جميع هذه الهواتف كانت تحمل رمز المنطقة 917 لتشارك دوائر نيويورك الخمس هذه الميزة)، وأمنت هذه الأعمال انطلاقة سريعة لصناعة الاتصالات المحتضرة في العراق عبر بناء البنية التحتية المادية المطلوبة، ليزدهر

هذا القطاع في غضون بضع سنوات.

وفي أفغانستان، حيث أسست الأمم المتحدة شبكة اتصالات نقالة مباشرةً بعد سقوط حكم طالبان (كخدمة مجانية لتشجيع المستخدمين)، نمت السوق نمواً ملحوظاً خلال العقد الماضي، ويعود الفضل في ذلك بشكل رئيس إلى قرار الحكومة الأفغانية المتمثل بمنح التراخيص لمشغلي الخدمة النقالة من القطاع الخاص. وبحلول عام 2011 كان هناك أربعة مشغلين رئيسين في أفغانستان يتقاسمون في ما بينهم 15 مليون مشترك، بعد أن كانت فرق إعادة الإعمار التي وصلت إلى العراق وأفغانستان قد وجدت أمامها صفحة بيضاء من البنى التحتية الفقيرة من دون مشتركين، وبإمكانيات تجارية غير واعدة. لكن، مع معدل انتشار الاتصالات النقالة حول العالم، وسرعة توسع صناعة الاتصالات، ليس من الوارد أن يجد أي شخص أمامه صفحة بيضاء بهذه الطريقة مرة أخرى.

أما في هاييتي، فبعد الزلزال الذي ضربها عام 2010 كانت المهمة الأساسية في مجال الاتصالات تتمثل في الترميم الشامل للبنية التحتية للاتصالات التي كانت متضررة تضرراً بالغاً. وعلى الرغم من الخراب الذي كان يعم البلاد، كانت استعادة شبكات الاتصالات وتشغيلها عملية سريعة نسبية. فقد كانت البنية التحتية للاتصالات النقالة متضررة على نحوٍ جسيم نتيجة الزلزال والهزات اللاحقة، لكن المشغلين - بفضل سرعة التفكير والتعاون بين شركات الاتصالات المحلية والجيش الأمريكي - تمكنوا من استعادة عمل الشبكات خلال بضعة أيامٍ فقط. فبعد عشرة أيام على الزلزال أفاد المشغلان الأساسيان للهواتف النقالةً، ديجي سيل وفوالا، أنه بات باستطاعتهما تشغيل 70 إلى 80 بالمئة من سعة ما قبل الزلزال.

يتذكر جيريد الذي كان وقتئذٍ يعمل مع وزارة الخارجية مساعدتَه السفير الأمريكي في أندونيسيا بعد وقت قصير على الزلزال في هاييتي. حيث كان يرغب بالاستفسار منه حول ما تعلّمه بعد تسونامي عام 2004 الذي تسبب بمقتل 230 ألف شخص في أربعة عشر بلداً في جنوب شرق آسيا، وكانت الرسالة واضحة: أعيدوا نصب الأبراج وتشغيلها، وأقنعوا أولئك الذين يعتقدون أن للاتصالات دوراً ثانوياً في عمليات الإنقاذ الطارئة أن الشبكات السريعة ليست ثانوية وإنما مكملة.

بما أن الغالبية العظمى من الأبراج الخلوية في هاييتي، حتى قبل الهزة الأرضية، كانت تعتمد على المولدات في عملها بدلاً من الكهرباء، فإن تأمين التغطية غالباً ما كان مسألة وقود أكثر من كونه مسألة بنية تحتية، كما كان لا بد من حراسة الأبراج التي تم التبرّع بها لمنع الناس القانطين من سرقة وقودها. إلا أن القدرة على تقديم هذه الخدمات على الرغم من الدمار والفوضى أثبتت أهميتها في عمليات التنسيق لإرسال منظمات الإغاثة إلى المناطق والبشر حيث تكون الحاجة إليها أكثر، إضافةً إلى توفير طريقة يتواصل من خلالها الأصدقاء وأفراد العائلة مع بعضهم داخل هاييتي وخارجها. كانت أولى الصور التي خرجت من البلاد بعد الكارثة بالفعل ملتقطة من قبل الهايتيين بواسطة هواتفهم النقالة، وأدرك كل من شارك في مرحلة ما بعد الزلزال الدور الحاسم للاتصالات وسط الدمار المادي المستشري والمعاناة الإنسانية.

كما أن الثورات التي بدأت في العالم العربـي عام 2010 مثال آخر جديد يبيّن منافع مبدأ . وليست مسارَعَة فودافون إلى إعادة الخدمة في مصر قبيل تنحي حسني مبارك سوى مؤشر على وجود قطاع اتصالات سريع الاستجابة ومتبصر. وقد أخبرنا فيتوريو كولاو من فودافون: "كان لدينا من ينام في مراكز الشبكة لضمان أن نكون أول من يقدم الخدمة بمجرد انتهاء وقف العمل بها. فقمنا بتأمين الطعام والشراب، واستأجرنا غرفاً في الفنادق القريبة، ووضعنا حراسة على مبانينا؛ لضمان عدم تعطيل الشبكة من قبل أي شخص". وبفضل هذه الجهود كانت فودافون أول مشغل يتابع تقديم خدمته، وتلك لحظة مهمة بالنسبة إلى شركة تسعى لأن تكون . فهي تحاول الوصول إلى السوق المصرية الكبيرة التي صار فيها فجأة الكثير مما يجب مناقشته. ووصف لنا كولاو استراتيجية ذكية متفهمة اتبعتها فودافون لتبين لزبائنها المصريين قيمتهم بالنسبة إليها: "منحنا زبائننا المصريين رصيداً يُمَكّنهم من الاتصال بأهلهم في المنـزل كهدية، كما قامت فودافون بتكييف الحمل على الشبكة (أي إنها أخلت مكاناً في الشبكة للمستخدمين المصريين)، "لكي نضمن أن يتمكن المستخدمون الأوائل لها - عند عودة الشبكة إلى العمل - من إجراء مكالمات بقيمة 20 يورو لطمأنة أقاربهم إلى أنهم بأمان".

يمثل الاعتماد على الاتصالات اليوم انعكاساً لمدى أهمية هذه التقانة التي أصبحت تتمتع بها حتى في أفقر المجتمعات. فعندما نتحدث اليوم عن استعادة الشبكة، غالباً ما نقصد تحديداً خدمات الصوت والتراسل النصي وليس الاتصال بالإنترنت، لكن ذلك سيتغير خلال العقد القادم مع اعتماد الناس في كل مكان على خدمات البيانات أكثر من اعتمادهم على الاتصالات الصوتية. فبعد الخروج من أزمة ما، ستكون الضغوط لاستعادة الاتصالات بالإنترنت أكبر بكثير من تلك التي نشهدها اليوم لاستعادة اتصالات الصوت والتراسل النصي. وكلاهما يصب في مصلحة الشعب، لأن شبكات البيانات السريعة ستساعد المشاركين في عملية إعادة الإعمار وفي تحقيق أهدافهم. وإذا لزم الأمر، فإن منظمات الإغاثة ستقوم بنشر أبراج نقالة من الجيل الرابع تتشابك مع بعضها لتشكل مزود خدمة إنترنت ذا عرض حزمة متدنٍ، حيث يمكن للبيانات أن تقفز من جهازٍ نقال إلى أقرب برج، ومنه إلى البرج التالي، إلى أن تصل إلى كابل من الألياف الضوئية متصل بالإنترنت الخارجية. وستكون سرعة التصفح متدنية، لكن مثل هذه التوزيعات ستؤمن ما يكفي من الاتصالات لتسريع عملية إعادة البناء.

ستكون الصدارة الخاصة التي تتمتع بها صناعة الاتصالات إحدى سمات النموذج الأولي لإعادة الإعمار. حيث ستكون شركات الاتصالات الوطنية في الصدارة بصفتها الكيانات الوطنية، أو كشريكة في التحالف مع القطاع الخاص. فشركة بشتل على سبيل المثال، وغيرها من الشركات الهندسية، كثيراً ما تُكلَّف بإعادة بناء البنى التحتية الفيزيائية عبر عقود حكومية، لكن مع تبني العالم مبدأ الاتصالات أولاً ستكون شركات الاتصالات هي أولى الشركات التي يرحَّب بها، وهي ستأتي، مثل غيرها، لجني المال. ستحتاج مجتمعات ما بعد الأزمة إلى الحصول على شبكات مستقرة بأسرع وقتٍ ممكن، لتنسيق جهود البحث والإنقاذ، ولإشراك الشعب،

ولحفظ حكم القانون، ولتنظيم عمليات توزيع المساعدات وتسهيلها، وللعثور على المفقودين، ولمساعدة أولئك المرحَّلين داخلياً على التنقل في بيئاتهم الجديدة. وستكون لشركات الاتصالات دوافع واضحة، ومشروعة تجارياً، لاستثمار مواردها في بناء شبكة اتصالات حديثة وصيانتها. وإذا تم تنظيم قطاع الاتصالات على نحو لائق منذ البداية، فسيعود ذلك بنفع جمعي كبير على جميع الأطراف؛ إذ ستجني الشركات عوائدها، وستتوفر للمشاركين في عملية إعادة الإعمار أدوات أفضل وأسرع، وسيتمكن الشعب بشكل عام من الوصول إلى خدمة موثوقة وسريعة ورخيصة (خصوصاً إذا كان القطاع تنافسياً منذ البداية).

أما فائدة وجود قطاع اتصالات صحي على المدى الطويل فتتمثل في دفعه للنمو الاقتصادي وتسهيله له؛ حتى حين تكون الطريق إلى الاستقرار طويلة. فالاستثمارات المباشرة في البنى التحتية بشكل عام توفر فرص العمل والخدمات للاقتصاد أكثر مما تقدمه برامج المساعدة قصيرة الأمد. وتعتبر الاتصالات أحد أكثر المشاريع ثباتاً على مستوى العالم في ميدان التجارة، وأكثرها درًّا للعوائد. فشركة روشان أكبر مشغل للهاتف الخلوي في أفغانستان، كما أنها أكبر مستثمر وأكبر دافع ضرائب في البلاد. فهي تشغل الآلاف في أفغانستان وتؤمن نحو 5 بالمئة من الناتج المحلي الكلي للحكومة الأفغانية؛ وذلك على الرغم من البنية التحتية الرديئة وانخفاض المداخيل، وبعد أكثر من عقد من الحرب المستمرة. أما في المستقبل، فسيدرك الفطناء من المشاركين في مشاريع إعادة الإعمار (من حكومات ومنظمات متعددة الجنسيات ومجموعات إغاثة) قيمة الاتصالات مباشرةً، وسيولون عملية بناء الشبكات الأولوية المناسبة بدلاً من اعتبار شركات الاتصالات منافسة لهم أو ضرورة قابلة للتأجيل.

ونظراً لكون الاتصالات قطاعاً رابحاً (وأشد ما تكون ربحيتها بعد أزمة ما؛ حين تكون مستويات النشاطات عاليةً على نحو غير اعتيادي)، ستتاح أمام المتعهدين المحليين والعالميين وفرة من الفرص يمكنهم المشاركة من خلالها. وسيستخدم المهندسون المحليون الموهوبون برمجيات مفتوحة المصدر لبناء منصاتهم الخاصة وتطبيقاتهم لمساعدة الاقتصاد الوليد، أو قد يتعاونون مع شركات ومنظمات خارجية ويساهمون بمهاراتهم. وسيكون جلّ الاستثمار في مجال الاتصالات عبارةً عن تعاملات بسيطة ومشاريع لتقديم خدمات مفيدة للناس. لكن، سيكون هناك خطر يتمثل في أن يكرس القادة التجاريون الذين سيبرزون حكماً أوليغارشياً، أو حكم قلة، رقمياً. وقد يكون هؤلاء القادة رجال أعمال محليين على علاقة وطيدة، يستغلون بيئة ما بعد الكارثة للسيطرة على صناعة أساسية، أو مديرين أجانب يسعون إلى توسيع إمبراطوريتهم. وسيكون التشريع مرةً أخرى هو المفتاح. فكما هو الحال في كل مشاريع إعادة الإعمار، سيكون على أولئك المسؤولين التيقظ لمثل هذه المحاولات في بيئة فوضوية ومرنة، وأن يستغلوا مواقعهم بشكلٍ فعال.

ستنضم إلى المتعهدين وأفراد القلة الحاكمة مجموعة من المستثمرين الأجانب، وأفراد من الجاليات في الخارج، وغيرهم من ذوي المصالح الشخصية، وليس المالية فقط. فالمستثمرون المتطلعون إلى الارتباط ببلدان جديدة سيجدون في

المستقبل أن إمكانيات الاتصال العالمية تنتج نوعاً جديداً من الارتباط أعمق وأكثر تعدداً للمظاهر. وستمنح تنبيهات الأخبار بالزمن الحقيقي، والشبكات الاجتماعية النشطة، والترجمة اللغوية الفورية، المستثمرين شعوراً بمزيد من القرب إلى البلدان التي يشتغلون فيها؛ تشبه المعرفة العميقة التي يمتلكها أبناء الجاليات في أنحاء العالم. وسيقود ذلك إلى استثمارات أفضل وأطول، وإلى علاقات مثمرة أكثر بالنسبة إلى المستثمرين، وكذلك بالنسبة إلى المجتمعات التي يتعاملون معها.

قلةٌ هم من يدركون ذلك أفضل من كارلوس سليم الحلو، قطب الاتصالات المكسيكي، وأغنى رجل في العالم حالياً. وسليم أحد أبناء الجالية اللبنانية التي تضم 15 مليوناً (كان أبوه قد هاجر من لبنان إلى المكسيك عام 1902 هارباً من الخدمة العسكرية في جيش الإمبراطورية العثمانية). ويدير سليم اليوم مصالح تجارية في أنحاء العالم عبر العديد من الشركات (منها حصة بمقدار 8 بالمئة في صحيفة نيويورك تايمز) وقد وصف لنا كيف ساهمت تجربته كابنٍ لمهاجرين في تشكيل رؤيته: "أعتقد أنني أشعر بأنني جزءٌ من العالم برمته أكثر من شعوري بأنني لبناني"، يقول لنا، "فأنا اليوم أشعر أنني في الوسط، بين لبناني ينتمي إلى التحديات القائمة هناك، ورجل أعمالٍ في أمريكا اللاتينية في الوقت نفسه؛ بما يمليه عليّ ذلك من مسؤوليات تجاه البلدان التي أدير فيها أعمالي".

ليس في تجربته شيء فريد كما يوضح لنا، بل إنه يتوقع أن الجميع في المستقبل سيكونون "أكثر عالميةً وأكثر محليةً"، مع تراكب الاهتمامات الإقليمية المتولدة عن إرث شخصي أو الناتجة عن فرص تجارية أو عن فضول محض. ويصف نفسه بأنه جزءٌ من مجموعة جديدة يسميها ، حيث يقول بصفته رجل أعمال عابراً للقوميات "إننا لا نتوجه إلى البلدان لمجرد ضخّ المال واستخراجه، بل نحن ندير الأعمال التجارية لكي نبقى ولنصبح جزءاً من التنمية في البلد. ربما ترى في ذلك شيئاً من ، لكنه أيضاً ذكاء تجاري. فالواقع يقول إن الأعمال تتحسن عندما تعمل على تنمية السوق وتنمية الطلب والزبائن والإمكانيات".

مع تراخي العراقيل التي تقف في طريق دخول الشركات الأسواق في عالم أكثر ترابطاً، لن تكون تجربة الانتماء إلى محصورة بأولئك القادرين على استثمار مبالغ كبيرة كرأس مال. فتخيل على سبيل المثال طالب معلوماتية في الهند يقوم بتطوير لعبة لشبكة اجتماعية ذات شعبية تشهد نجاحاً مفاجئاً بين المستخدمين في سيريلانكا. ربما لا يكون لدى هذا الطالب والمتعهد الملهم جواز سفر (وقد لا يعلم أي شيء عن سيريلانكا)، لكن لعبته تصبح مربحة جداً هناك - أياً كانت الأسباب - مما يثير فضوله، فيضيف أصدقاء سيريلانكيين على الفيسبوك وغوغل+، ويتابع الأخبار المحلية على تويتر، ويبدأ بالتعرف على البلد، ثم يسافر إليه. وسرعان ما يطور علاقة قرابة رقمية مع البلد ستدوم لسنوات قادمة. هذا ما سيعيشه الملايين من المتعهدين ومطوري التطبيقات ورجال الأعمال في المستقبل، لأن الأسواق على الشبكة ستكون أكبر وأكثر تنوعاً مما يمكن لأي شخص أن يتخيله حقاً.

ستكون هذه النظرة في إطار إعادة الإعمار مشجعة بالطبع، لكن معظم

شركات الاتصالات، حتى أكثرها تنظيماً وحسن نية، لن تتمكن أبداً من تقديم بديل عن العمل الجبار للمؤسسات الحكومية. فثمة سلع وخدمات اجتماعية أساسية لا يستطيع أحد تقديمها للشعب سوى حكومته؛ كالأمن وبرامج الصحة العامة والمياه النظيفة وبنية المواصلات التحتية والتعليم الأساسي، ومن شأن الاتصالات وإمكانيات التواصل أن تحسن فعالية هذه الوظائف، لكن ذلك لن ينجح سوى في إطار شراكة مع الفاعلين المؤسساتيين على الأرض كما يبين المثال التالي.

مع انهياره الأول عام 1991 أصبح الصومال أول دولة فاشلة في العالم. وباتت المجاعات وحرب العشائر والاعتداءات الخارجية والتمردات الإرهابية تُعجِز الحكومات الانتقالية؛ الواحدة تلو أخرى. لكن، خلال السنوات الأخيرة، كان تنامي الهواتف الخلوية في الصومال أحد النجاحات القليلة التي برزت في معمعة الفوضى. فحتى مع انعدام الأمن وغياب حكومة قادرة على القيام بوظائفها، قامت صناعة الاتصالات بدور حيوي في الكثير من جوانب المجتمع، فكانت تؤمن للصوماليين فرص العمل والمعلومات والأمن والاتصالات الهامة بالعالم الخارجي، بل إن شركات الاتصالات هي في الحقيقة الشيء الوحيد المنظم في الصومال، فهي تتجاوز الديناميات العشائرية والقبلية وتعمل عبر المناطق الثلاث: جنوب وسط الصومال (مقاديشو)، وأرض البنط في الشمال الشرقي، وأرض الصومال في الشمال الغربـي. ويوجد في الصومال مصرف تجاري واحد (تم تأسيسه في أيار عام 2012). وقبل أن تتوفر الهواتف الخلوية، كان الصوماليون يعتمدون في تحريك الأموال على شبكات الحوالات غير الرسمية التي لا تحتفظ بأية سجلات لمناقلاتها. أما اليوم، فقد صارت خدمات تحويل الأموال النقالة تسمح لمئات الآلاف من الصوماليين بتحويل الأموال داخل البلاد وبتلقي الحوالات من الخارج. وثمة منصات تعتمد على الرسائل القصيرة، وتسمح للمشتركين باستخدام البريد الإلكتروني وباستقبال النصائح المتعلقة بالأسهم ومعلومات الطقس.

تطلق الشركات والمنظمات غير الحكومية الأجنبية بانتظام مشاريع تقانة نقالة تجريبية لتحسين الفرص المتاحة أمام الشعب الصومالي بطرق بسيطة. وقد شهدنا محاولات لبناء منصات بحث عن فرص عمل تعتمد على الرسائل النصية القصيرة ونظم الرعاية الصحية النقالة للتشخيص عن بعد، بالإضافة إلى مشاريع أخرى. إلا أن معظمها فشلت في تثبيت أقدامها على الأرض، ولا غرابة في ذلك نظراً إلى البيئة العدوانية على نحو استثنائي من الناحيتين الأمنية والتجارية. لذا، إنّ معظم الإبداعات التي تصلنا من الصومال اليوم تأتي من الصوماليين أنفسهم، وهو ما يحدث في أماكن أخرى من العالم النامي، فمعظم الحلول المبتكرة تبزغ من المستوى المحلي مدفوعة بالضرورة قبل أي شيء آخر.

أدى غياب الحكومة في الصومال إلى قطاع اتصالات غير منظم شجع على انخفاض الأسعار لأنه يمكن للمتعهدين الجدد أن يدخلوا السوق ويقيموا شبكاتهم إذا رأوا فرصة سانحة للربح (وتوفرت لديهم الرغبة الكافية للمجازفة). وهذا نموذج يتكرر حين يتوقف عمل الحكومة. ففي الأسابيع التي تلت سقوط صدام حسين، حاولت شركة اتصالات بحرينية التوسع في جنوب العراق واستغلال الروابط

الطائفية بين تلك المنطقة، لكسب الزبائن. لكن قوات الاحتلال العسكرية، التي خشيت من إلهاب التوترات الطائفية، حالت دون تمام المشروع في النهاية.

أنتجت بيئة الأعمال المفرطة في تراخيها في الصومال بعض أرخص رسوم الاتصالات المحلية والدولية واتصالات الإنترنت، مما جعل استخدام الهواتف النقالة أيسر بكثير بالنسبة إلى الشعب الذي يعيش في فقر مدقع. فعندما يتصل أبناء الجالية الصومالية في الولايات المتحدة بأقاربهم في الوطن، غالباً ما يغلق أقاربهم الخط ويعاودون الاتصال بهم. وفي غياب حكومة تفرض الضرائب وتتقاضى رسوماً لقاء التراخيص التي تمنحها أو تفرض تكاليف تنظيمية، تستطيع شركات الاتصالات إبقاء تكاليفها منخفضة وتوسيع قاعدة مشتركيها وتحقيق الربح في الوقت نفسه. فانتشار الهاتف النقال في الصومال أعلى بكثير مما قد يتوقع المرء، حيث يتراوح بين 20 و25 بالمئة. ويقدم المشغلون الرئيسون الأربعة للاتصالات الخدمات الصوتية وخدمات البيانات في جميع أنحاء البلاد، وضمن حزام بعرض ستين إلى سبعين ميلاً ضمن الأراضي الكينية المجاورة أيضاً.

على الرغم من الإنجازات التي تم تحقيقها في مجال الاتصالات، يبقى الأمن في الصومال مفقوداً على نحو خطير. فقد استخدم المتمردون الاتصالات المتوفرة في البلاد للتمادي في عنفهم، إذ يرسل متمردو حركة الشباب الإسلامي تهديداتهم إلى عناصر قوات حفظ السلام التابعة للاتحاد الأفريقي هاتفياً أو عبر الرسائل القصيرة. ويحظرون منصات الصيرفة النقالة، ويخربون البنية التحتية للاتصالات. ويستخدم القراصنة على السواحل الصومالية شبكات الاتصالات المحلية للتواصل لأنهم يخشون من تتبع هواتفهم الفضائية من قبل السفن الدولية. وفي تقرير له في شباط عام 2012 أضاف مجلسُ الأمن رئيسَ شركة هرمود، أكبر شركة اتصالات في الصومال، إلى لائحة الأفراد المحظورين من السفر بعد التثبت من أنه أحد كبار الممولين لحركة الشباب (وورد في التقرير أيضاً أن علي أحمد نور جمالي قد أعد نظام تحويل الأموال النقال التابع لشركة هرمود بهدف تسهيل التمويل مغفل الهوية لحركة الشباب).

لا شك في أن الموقف في الصومال معقد. لكن، إذا استطاعت البلاد الخروج من دوامة الفوضى في وقت قريب، فستجد الحكومة الجديدة بالتأكيد من يرغب بمشاركتها بين مشغلي الاتصالات الوطنيين.

في الحالة المثالية، ستسعى مشاريع إعادة الإعمار ليس فقط إلى إحياء ما كان موجوداً فقط، بل وإلى تحسين الأصيل وتطوير سلوكيات ومؤسسات تخفف خطر تكرار الكارثة. فلدى معظم مجتمعات ما بعد الأزمة - وإن تنوعت من حيث التفاصيل - الحاجات الأساسية نفسها التي تشبه بدورها المكونات الأساسية لعمليات بناء الدولة من سيطرة إدارية على الأرض، واحتكار لأدوات العنف، وإدارة سليمة للمالية العامة، واستثمار في رأس المال البشري، وضمان جاهزية البنية التحتية، واستحداث حقوق المواطنة وواجباتها*. ويجب أن تقود دولة ما بعد الأزمة بنفسها المحاولات الرامية إلى تلبية هذه الحاجات، وإن كانت هذه تعتمد اعتماداً كبيراً على المجتمع الدولي (مالياً وتقنياً ودبلوماسياً). فحين لا تكون مشاريع إعادة

الإعمار وليدة البلد، أو على الأقل منسجمة مع التطلعات السياسية والاقتصادية للمجتمع، فسيرتفع احتمال الفشل ارتفاعاً هائلاً.

ستساعد التقانة على حماية حقوق الملكية وحراسة السجلات الافتراضية للأصول حيث يمكن استعادة هذه الأصول بسرعة عندما تستقر الأمور. فليس من الوارد أن يضع المستثمرون أموالهم في بلد لا يمنحهم الطمأنينة في ما يتعلق بأمنهم وملكية أصولهم. وقد أُنشئت في عراق ما بعد الغزو ثلاث لجان تسهل على السكان المحليين والعائدين من المنفى المطالبة بممتلكاتهم التي تم الاستيلاء عليها في زمن نظام صدام حسين أو تلقي تعويضات عنها، كما وعينت هيئة موازية لحل النـزاعات. وكانت تلك الخطوة هامة جدًّا في ما يتعلق بعملية إعادة الإعمار في العراق، فقد ساعدت على التخفيف من مظاهر استغلال فوضى ما بعد الحرب ومن حالات انتزاع الممتلكات بالقوة. لكن، على الرغم من حسن نوايا هذه اللجان (تم تلقي أكثر من 160,000 طلب حتى عام 2011)، فإن عملها كان يتعثر نتيجة القيود البيروقراطية التي تزج الكثير من الطلبات في عمليات تقاضٍ معقدة. أما في المستقبل، فستتعلم الدول من النموذج العراقي أن توفر حماية أكثر شفافية، وأمناً لحقوق الملكية من شأنه أن يمنع مثل هذه المشاحنات في حال نشوب نـزاع. فعبر إنشاء نظم مساحية شبكية (نظم سجلات شبكية تحوي أسعار الأراضي وحدودها على سبيل المثال)، مع برمجيات للخرائط يمكن استخدامها من الهواتف النقالة، تستطيع الحكومات تمكين مواطنيها من الاستعراض الرسومي لجميع الأراضي العامة والخاصة، بل ورفع الشكاوى الصغرى - مثل خلاف على سياج - إلى وسيط مُجاز على الشبكة.

لن يكتفي الناس في المستقبل بإجراء نسخ احتياطي لبياناتهم، بل سيجرون نسخاً احتياطية لحكوماتهم أيضاً. فضمن النموذج الأولي الناشئ لإعادة الإعمار، ستكون المؤسسات الافتراضية قائمة على التوازي مع قرينتها المادية، وستلعب دور النسخة الاحتياطية وقت الحاجة. فبدلاً من أن يكون هناك بناءٌ مادي للوزارة تُحفظ فيه جميع السجلات، وتقدم منه جميع الخدمات، ستكون هذه المعلومات مرقمنةً ومخزنةً في السحابة. وسيتم تنفيذ الكثير من الوظائف الحكومية عبر منصات شبكية. فإذا تسبب تسونامي بتدمير المدينة على سبيل المثال، فستستمر جميع الوزارات في عملها بقدر معين من الكفاءة في العالم الافتراضي، بينما تكون عملية إعادة إعمارها جارية على قدم وساق في العالم المادي.

ستسمح المؤسسات الافتراضية للحكومات الخارجة من الصدمة حديثاً بالحفاظ على الكثير من فعاليتها في تقديم الخدمات، إضافة إلى صيانة الدور الهام الذي تلعبه هذه الحكومات في مشاريع إعادة الإعمار كلها. ولن تستطيع المؤسسات الافتراضية القيام بكل شيء كانت تستطيع القيام به في الظروف العادية، لكنها ستقدم مساعدة هائلة. فسيحتاج قسم الخدمات الاجتماعية المسؤول عن توزيع الملاجئ في النهاية إلى مراسلين ميدانيين يتفاعلون مع الناس، لكنه سيستطيع - مع توفر المزيد من البيانات - توزيع الأسرّة توزيعاً أكثر فعالية، وتتبع الموارد المتوفرة، إضافة إلى القيام بمهام أخرى. وإذا كان الجيش الافتراضي لا يستطيع

فرض حكم القانون، فإنه يستطيع ضمان استلام عناصر الجيش والشرطة لمستحقاتهم مما سيخفف بعض المخاوف. وعلى الرغم من أن الحكومات ستبقى متوجسةً بعض الشيء من ائتمان مزودي خدمات السحابة على بياناتها، فإن الطمأنينة التي تضمنها لها النسخ الاحتياطية لمؤسساتها ستكون مبرراً كافياً لإنشائها.

وستؤمن هذه المؤسسات شبكة أمان للشعب أيضاً، فهي تضمن الحفاظ على السجلات وتسديد أرباب العمل للرواتب وصيانة قواعد بيانات المواطنين؛ داخل البلاد وخارجها على حدّ سواء. وسيسرع كل ذلك المساهمة المحلية في عملية إعادة الإعمار، وفي الحد من الهدر والفساد اللذين يتبعان عادة الكارثة أو النـزاع. فالحكومات قد تنهار، والحروب قد تدمر البنى التحتية المادية، لكن المؤسسات الافتراضية ستنجو.

سيكون بإمكان حكومات المنفى أن تعمل بطريقة مختلفة تماماً عما أتيح لحكومات بولندا وبلجيكا وفرنسا التي أجبرت على العمل من لندن خلال الحرب العالمية الثانية. فنظراً إلى جودة الأداء التي ستتمتع بها المؤسسات الافتراضية، ستعمل الحكومات المستقبلية عن بعد مع مستوى من الفعالية ومدى الوصول لم يشهد له مثيل من قبل. ستكون هذه الحركة وليدة الضرورة؛ إما بسبب كارثة طبيعية، أو بسبب شيء أطول أمداً كالحرب الأهلية. فتخيل أن تصبح مقديشو فجأة مناوئة لحكومة الصومال المحاصرة على نحو يمنع الحكومة من العمل؛ ربما بسبب استيلاء متمردي الشباب على المدينة، أو لأن الحرب العشائرية جعلت البيئة في المدينة غير قابلة للسكن. عندها، يمكن لمسؤولي الحكومة - إذا كانت المؤسسات الافتراضية قائمة - أن ينتقلوا مؤقتاً داخل البلاد أو خارجها مع حفاظهم على شكل معين من السيطرة على الإدارة المدنية للدولة. وأقل ما يمكنهم فعله هو الحفاظ على مستوى من المصداقية لدى الشعب عبر ترتيبهم عملية توزيع الرواتب، والتنسيق مع منظمات الإغاثة والمانحين الأجانب والتواصل مع الجمهور تواصلاً شفافاً. ولن يكون الحكم الافتراضي الذي يمارس عن بعد في مطلق الأحوال سوى مخرج نهائي بالطبع (فلا شك في أن المسافة ستغير مقدار مصداقية الحكومة وإمكانية محاسبتها في أعين مواطنيها)، لذا لا بد من تحقق بعض الشروط المسبقة لكي ينجح مثل هذا النظام؛ كتوفر شبكات سريعة وموثوقة وآمنة، ومنصات متطورة، وإمكانيات تواصل كاملة لدى الشعب. وما من دولة مستعدة لتوفير كل ذلك اليوم (وأقلها استعداداً لذلك هي الصومال)، لكن البلدان إذا شرعت ببناء مثل هذه الأنظمة الآن فستجدها جاهزةً عندما تحتاج إليها.

ربما تؤثر الإمكانيات التي يطرحها الحكم الافتراضي عن بعد تأثيراً كبيراً على سياسيي المنفى، فبينما كان على الشخصيات العامة المقيمة خارج أوطانها ذات يوم أن تعتمد على قنوات خلفية لتبقى على تواصل مع بلدانها (ومن المعروف أن آية الله الخميني كان يعتمد على تسجيلات صوتية على شرائط كاسيت تسجل في باريس وتُهرَّب إلى إيران لكي ينشر رسالته في سبعينيات القرن العشرين)، ثمة اليوم طيف واسع من البدائل الأسرع والأكثر أماناً وفعالية سيسمح لسياسيي

المنفى في المستقبل بتشكيل مؤسسات افتراضية قوية من شأنها التغطية على الحكومات بشكلٍ كامل، ويمكنهم عبرها التفاعل مع حاجات الشعب في الوطن وتلبيتها.

وليس في ما سبق مبالغة كما يبدو للوهلة الأولى. فبفضل الاتصالات، سيكون المقيمون في المنفى أقل غربة عن شعوبهم مقارنةً بأسلافهم. ومع تأقلمهم الدقيق مع توجهات أوطانهم وأمزجتها، سيكون بمقدورهم توسيع مداهم وأثرهم بين الجمهور عبر رسائل موجهة من خلال منصات وأجهزة بسيطة وشعبية. ولن يكون على قادة المنفى أن يركزوا على مكان معين لتشكيل حزب أو حركة، فالفروقات الهامة بين الأماكن ستكون إيديولوجية وليست جغرافية. عندما تتوفر للمقيمين في المنفى منصة متماسكة، ورؤية لمستقبل البلاد، سيكون بإمكانهم إيصال خططهم إلى الشعب في الوطن بسرعةٍ وأمان من دون أن يكونوا قد وضعوا أقدامهم في البلاد من قبل، وسيوصلون ملايين النسخ من هذه الخطط؛ حيث تعجز الحكومة الرسمية عن إيقاف هذا التدفق.

سيستخدم المقيمون في المنفى المؤسسات الافتراضية التي يسيطرون عليها لكسب عقول وقلوب شعبهم. فتخيل حكومة ظل تموِّل وتنشر قوى أمنية داخل البلاد تضم في صفوفها أبناء جنسيات أجنبية مختلفة لحماية معاقلها، بينما تقدم خدمات رعاية صحية إلكترونية من باريس (مع إدارات مشافٍ مستقلة تنظم حملات تلقيح مجانية، وتوسِّع خطط التأمين الصحي الافتراضية، وتنسِّق شبكة من الأطباء العاملين عن بعد تقدم خدمات تشخيصية)، وتدير مدارس وجامعات على الشبكة من لندن. تستطيع حكومة منفى كهذه انتخاب برلمانها الخاص حيث تشن الحملات الانتخابية ويجري التصويت على الشبكة بشكلٍ كامل. حينها سيكون أعضاؤها من بلدان مختلفة، وستتم إدارة جلساتها عبر قنوات الفيديو الحي التي يمكن للملايين مشاهدتها حول العالم. وقد يكفي توفر حكومة ظل وظيفية - ولو بمظهرها الخارجي - لدفع الناس في الوطن إلى تحويل دعمهم من الحكومة الرسمية إلى تلك التي يتم بناؤها وتشغيلها عن بعد من المنفى.

تبقى هناك سمة مميزة أخرى بعد للنموذج الأولي لإعادة الإعمار؛ ألا وهي انخراط جاليات الشتات في هذه العملية عن كثب. فغالباً ما تتشكل حكومات المنفى من مثقفي الشتات، لكن دور الجاليات الخارجية لن يكون سياسياً أو مالياً (على شكل حوالات) فقط، لأن توفّر الاتصالات يعني أن هذه المجموعات ستتمكن من العمل معاً على مسافة أقرب لمعالجة طيف أوسع من المسائل. وأبناء الجاليات في الخارج يتمتعون بالتبصر وبمعرفة عميقة لا تقدر بثمن في سياق إعادة الإعمار. ومع توفر المزيد من تقانات الاتصالات، ستتمكن مجتمعات ما بعد الأزمة من أن تنهل من موارد رأس المال البشري العظيمة هذه. لقد سبق أن شهدنا مؤشرات على ذلك في الأزمات الأخيرة التي شهدها العالم، فقد استخدم أبناء الجاليات الصومالية أدوات مثل غوغل ماب ميكر بفعالية لتحديد المناطق المتأثرة بالقحط الذي اجتاح القرن الأفريقي عام 2011؛ مستخدمين معرفتهم بالمكان واتصالاتهم المحلية لجمع تقارير أكثر دقة مما يستطيع العاملون الخارجيون جمعه.

سنشهد في المستقبل موارد بشرية احتياطية في الشتات تضم أولئك الذين يعيشون في الخارج بعد تنظيمهم وفقاً لمهنهم؛ من أطباء وضباط شرطة وعمال بناء ومدرسين وما إلى ذلك. وسيكون على الدول تنظيم أبناء جالياتها (على فرض أن هذه الجاليات ليست كلها من المنفيين السياسيين المعادين للدولة)، حيث تعلم من يمتلك المواهب التي قد تتطلبها البلاد وقت الحاجة. فالعديد من الجاليات تتمتع اليوم بمستوى من النجاح أعلى مما تحققه شعوبها في أوطانها الأم (وينطبق ذلك على الجاليات الإيرانية والكوبية واللبنانية، لكن أيضاً على مجموعات أصغر كالصوماليين وأبناء قومية الهمونغ). لكن شرائح معينة فقط من هذه الجاليات لا تزال على تواصل مع بلدانها الأم، فالكثير من أبنائها اندمج - عمداً أو بفضل عامل الزمن - في البلدان المختارة لما تقدمه من فرص وأمان وجودة حياة. ومع انتشار الاتصالات، ستتقلص الفجوة التي تفصل بين أبناء الشتات ومجتمعات الوطن مع تقوية تقانات الاتصالات والوسائط الاجتماعية للصلات الثقافية واللغوية والرؤيوية التي تربط هذه المجموعات المتباعدة. أما أولئك الذين سيغادرون بلدانهم كجزء من هجرة الأدمغة في المستقبل، فسيغادرون بلداناً أكثر تواصلاً بكثير مما هي اليوم، حتى إذا كانت تلك الأماكن تعاني من الفقر أو الاستبداد أو من غياب الفرص. وسيكون بمقدور أبناء الجاليات عندها إنشاءُ اقتصاد معرفي في المنفى ينهل من المؤسسات التعليمية القوية والشبكات والموارد في البلدان المتطورة، وضخّ ثمارها على نحو بنّاء إلى الأوطان.

الانتهازية والاستغلال

عقب كل نـزاعٍ كبير أو كارثة طبيعية يفيض المكان بالفاعلين الجدد من عمال إغاثة، وصحفيين، ومسؤولي الأمم المتحدة، ومستشارين، ورجال أعمال، ومتفرجين، وسياح. بعضهم يأتي لعرض خدماته، بينما يأتي آخرون على أمل استغلال بيئة الأزمة لتحقيق مكاسب سياسية أو اقتصادية، والكثيرون يأتون لتحقيق الغرضين معاً؛ وهو الخيار الأكثر فعالية*.

حتى إن أولئك الذين لا يبغون ربحاً مالياً، تكون لديهم أسباب تدفعهم للمشاركة لا تقف عند الإيثار. فبلدان ما بعد الأزمات تعتبر أرض امتحان ممتازة للمنظمات غير الحكومية الناشئة، ومسرحاً يمكن فيه للمنظمات غير الربحية الراسخة أن تستعرض قيمها أمام المانحين. قد يترافق هذا التدافع للمشاركين الجدد (الغيريين والانتهازيين على حدٍّ سواء) مع خير وفير أو ضرر هائل. وسيكون التحدي القائم أمام مخططي عملية إعادة الإعمار في المستقبل هو إيجاد طرق للموازنة بين مصالح جميع الأشخاص والمجموعات وأفعالهم بطريقة منتجة.

إذا ابتغينا التعميم، فإن انتشار الاتصالات يشجع سلوك الإيثار ويسهِّل اتباعه. فهو يجعل الناس أكثر اطلاعاً على معاناة الآخرين وأكثر إدراكاً لها، ويمنحهم المزيد من الفرص لفعل شيء حيالها. وقد يسخر البعض من (أي المنخرطين في فعاليات اجتماعية بقدر قليل من الجهد أو من دون جهد على الإطلاق)، لكن المنظمات العابرة للجنسيات، والتقدمية في تفكيرها - مثل كيفا وكيك.ستارتر -

تعطي فكرة عما سيكون عليه مستقبلنا المتواصل. فكيفا وكيك.ستارتر منصتان للتمويل الجماهيري (حيث تركز كيفا على التمويل الصغري، بينما تركز كيك.ستارتر بشكلٍ رئيس على المشاريع الإبداعية)، بينما تعمل منصة ساماسورس على تعهيد التي تحتاج إليها الشركات إلى أشخاصٍ في البلدان النامية عبر منصاتٍ شبكية بسيطة. وبعيداً عن التبرع بالمال، ثمة طرقٌ أخرى - أقل قابلية للقياس - للمساهمة في دعم قضية ما عن بعد، مثل إنشاء المحتويات الداعمة، أو زيادة وعي الجماهير بالقضية، وكلاهما يشكلان جزءاً متكاملاً أكثر فأكثر من هذه العملية.

مع اتصال المزيد من الناس حول العالم سنشهد تكاثراً للمتبرعين المحتملين والناشطين المستعدين للمساهمة خلال الأزمة الكبرى التالية. ومع ازدياد إمكانية الوصول بالزمن الحقيقي إلى معلومات حول الصراعات والكوارث حول العالم، وانتشارها بالتساوي على منصات مختلفة بلغات متنوعة، سيُسمع صدى أزمة في بلد ما في جميع أنحاء العالم حال حدوثها. ولن تحفز الأخبار كل من يتلقاها على المبادرة للقيام بأمرٍ ما، لكن عدداً كافياً من الناس سيبادرون؛ مما يوسع نطاق المشاركة توسيعاً هائلاً.

إن إلقاء نظرة عن كثب على ما حدث بعد زلزال هاييتي مرة أخرى يقدم لنا أدلّة جيدة عما يحمله لنا المستقبل. فقد كان مستوى الدمار بالقرب من العاصمة الهاييتية - البلد كثيف السكان ومدقع الفقر - ساحقاً. فقد كانت المنازل والمستشفيات وأبنية المؤسسات قد انهارت، ونظم المواصلات والاتصالات قد دمرت، ومئات الآلاف من البشر قد قضوا نحبهم، بينما أصبح 1.5 مليون شخص في عداد المشردين. ولم تمض ساعات قليلة حتى كانت الحكومات المجاورة قد أرسلت فرق خدمات الطوارئ. وخلال بضعة أيام، كانت دول كثيرة من مختلف أنحاء العالم قد تعهدت بإرسال المساعدات أو أرسلتها بالفعل*.

وجاء رد الأوساط الإنسانية أقوى بعد، فبعد أيام من الزلزال كان الصليب الأحمر قد جمع أكثر من خمسة ملايين دولار عبر حملة تسمح لمستخدمي الهواتف النقالة بإرسال رسالة نصية تحتوي كلمة إلى رمز قصير خاص (90999) للتبرع بعشرة دولارات تُحمَّل آلياً على فاتورة هاتفه. ووفقاً لمؤسسة موبايل غيفنغ التي تنشئ البنى التحتية التقنية التي تستخدمها الكثير من المنظمات غير الحكومية، فقد مر ما مجموعة 43 مليون دولار من المساعدات عبر منصات التبرع النقالة. وقامت منظمة اتصالات بلا حدود - وهي منظمة إنسانية متخصصة في اتصالات الطوارئ - بالانتشار على الأرض في هاييتي بعد الزلزال بيوم واحد، وأقامت مراكز اتصال تسمح لأفراد العائلات بالوصول إلى أحبتهم. وبعد مرور خمسة أيام على الزلزال فقط، كانت خدمة الأخبار الإنسانية ألارت.نت التابعة لمؤسسة تومسون رويترز قد أعدت "خدمة معلومات الطوارئ" الأولى من نوعها لتسمح للهاييتيين بإرسال رسائل تحذير قصيرة مجانية تساعدهم على السيطرة على آثار الكارثة.

تحولت عمليات الإغاثة الطارئة إلى مشاريع إعادة إعمار طويلة الأمد. فخلال

بضعة أشهر، كانت عشرات الآلاف من المنظمات غير الحكومية قد شرعت بالعمل الميداني في هاييتي. ومن الصعب تخيل عشرات الآلاف من المنظمات تعمل على نحوٍ فعالٍ (بأهدافٍ واضحة وغير متكررة) في مكانٍ واحد، ناهيك عن عملها في بلد صغير جداً ومزدحم ومتنوع مثل هاييتي. وبمرور الشهور، بدأت تطفو على السطح تقارير مقلقة حول عدم فعالية توزيع المساعدات، فكانت المخازن متخمةً بالمستحضرات الصيدلانية غير المستخدمة التي تُركت بسبب سوء الإدارة فيما تاريخ انتهاء صلاحيتها يقترب، وبات تفشي الكوليرا في المستعمرات غير الرسمية المتكاثرة يهدد بحصد أرواح الناجين من الزلزال. وكان توزيع التمويل القادم من متبرعين مؤسساتيين - معظمهم من الحكومات - متلكئاً وصعب المتابعة. ولم يكن يصل إلى الهاييتيين أنفسهم سوى النـزر اليسير من هذا التمويل بعد أن يكون الباقي قد انتهى بين يدي إحدى المنظمات الأجنبية ذات الموقع الأعلى في هذه السلسلة. وبعد مرور عام على الزلزال، كان مئات الآلاف من الهاييتيين ما زالوا يعيشون في مدن من الخيام غير صحية بسبب عدم تمكن الحكومة وشركائها من المنظمات غير الحكومية من إيجاد طريقة أخرى لإيوائهم. وبعد كل تلك التغطية وجمع التبرعات وخطط التنسيق والنوايا الحسنة، لم تلبَ حاجات الهاييتيين كما يجب في بيئة ما بعد الزلزال.

ثمة أشخاص يمتلكون من المؤهلات ما يخولهم عن جدارة تقديرَ ما كان يجري في هاييتي، وقد قاموا بالتدقيق في هذه النتائج بحرص كبير (منهم باول فارمر في كتابه **هاييتي بعد الزلزال**). ويبدو أنه ثمة إجماع على أن عوامل عدة مؤسفة قد اجتمعت هناك. فجاء الدمار الشامل مصحوباً ببيروقراطية معدومة الكفاءة على خلفية من التحديات القديمة المستحكمة بعمق. وما كان لتقانات الاتصالات أن تأمل في التخفيف من مصائب هاييتي. لكن المنصات الشبكية المنسقة، إذا استُغلّت بشكل صحيح وعلى نطاق واسع، تستطيع ضبط هذه العملية في كثير من المجالات حيث تؤدي النسخة المستقبلية من زلزال هاييتي إلى قدر أكبر من النتائج الجيدة، وإلى قدر أقل من الهدر، وإلى فترة نقاهة أقصر. سنستعرض خلال هذا القسم بعض أفكارنا الخاصة، مع إدراكنا التام أن الفاعلين المؤسساتيين (أي المنظمات غير الحكومية الكبيرة، والحكومات الأجنبية المانحة وغيرها) ربما لن يكونوا مستعدين، في ظروف إعادة الإعمار، لاتخاذ هذه الخطوات خوفاً من الفشل أو من فقدان النفوذ في المستقبل.

حين نفكر في الموجة التالية من الكوارث والنـزاعات التي ستطرأ في عصر أكثر تواصلاً، يمكننا تلمس نموذج متكرر قيد النشوء. فتوافر المزيد من المانحين المحتملين، إضافة إلى إمكانية التسويق المدهشة على الإنترنت، سيؤديان إلى التي تظهر في كل مجتمع خارج من أزمة. وستنفجر
هذه الفقاعة في النهاية لتقود إلى قدر أكبر من اللامركزية في عمليات الإغاثة، وإلى موجة من التجارب الجديدة.

كانت منظمات الإغاثة الراسخة تتميز في ما بينها تاريخياً باسمها أكثر من تميزها بتأثيرها. فالشعارات الجذابة، والإعلانات المؤثرة، والتزكيات الوجاهية لها أثر أكبر

بكثير في جذب التبرعات العامة مقارنةً بالتقارير المفصلة عن السّوقيات وشبكات الأسرّة الحامية من الملاريا والنجاحات المتراكمة. وربما ما من مثال حديث أفضل من فيديو "كوني 2012"، الذي أصبح سيئ الصيت اليوم، والذي أنتجته منظمة

غير الربحية للتوعية في ما يتعلق بأوضاع الحرب التي استمرت لعقودٍ عدة في شمال أوغندا. فبينما كانت مهمة المنظمة المتمثلة بإنهاء الفظاعات التي كانت ميليشيا الأوغندية ترتكبها مهمةً نبيلة، وجد الكثيرون من العارفين بالنـزاع عن قرب (ومنهم الكثيرون من الأوغنديين) الفيديو مضللاً ومبسطاً ويخدم في النهاية مآرب ذاتية. إلا أن الفيديو حصد أكثر من 100 مليون زائر في أقل من أسبوع (ليكون أول فيديو فيروسي يصل إلى هذا الرقم)، ويعود الفضل الأكبر في ذلك إلى تزكياتٍ حملت تواقيع مشاهير بارزين لديهم الملايين من المتابعين على تويتر، ولم تنفع الانتقادات المبكرة للمنظمة وعملياتها (مثل أعباء تكاليف الإنتاج التي بلغت نسبتها سبعين بالمئة لديها، وما هي في الحقيقة سوى الرواتب) في كبح التيار الهائج؛ إلى أن انتهى الأمر فجأةً مع الاعتقال العلني جداً، والغريب، لأحد مؤسسي المنظمة بعد أن كشف أمره على الملأ.

كما ذكرنا سابقاً، سنشهد ميداناً للتسويق أكثر استواء في الحقبة الرقمية؛ فبإمكان أي شخص يمتلك منظمةً غير حكومية مسجلة أو جمعيةً خيرية (أو حتى من دون هذه الأخيرة) أن يعدّ منصة شبكية مبهرجة، مع محتوى عالي الجودة وتطبيقات نقالة جذابة؛ فهذه في النهاية أسرع وأسهل طريقة يكرس بها فرد أو مجموعة علامته. أما الجوهر الفعلي للمنظمة (أي مدى ضلوعها وكفاءتها وكيفية تعاملها مع الإيرادات ومدى جودة برامجها أو رداءتها)، فهو أقل شأناً. وعلى غرار ثوار المشروعات الناشئة الذين يولون المظهر قيمةً أعلى مما يولون الجوهر، سيتوصل المشاركون الجدد إلى طرائق يستغلون بها النقاط العمياء لدى داعميهم. ويمكن لهذه المجموعات في هذه الحالة أن تستغل حقيقة أن المتبرعين على قدر ضئيل من الاطلاع على ما يجري في الميدان. وعندما تضرب كارثة وتتدفق المنظمات غير الحكومية إلى المكان، ستجد المنظمات الراسخة منها نفسها جنباً إلى جنب مع منظمات ومجموعات ناشئة تتمتع بحضورٍ قوي على الشبكة وتمويل أوّلي، لكنها بشكلٍ عام لم تخضع للاختبار. وستكون مثل هذه المنظمات الناشئة أدق تصويباً في مهمتها مقارنةً بمنظمات الإغاثة التقليدية، وستبدي القدر نفسه من الكفاءة، إن لم يكن أكثر، مقارنةً بقريناتها من المنظمات الراسخة. وستتمكن من جذب الاهتمام، لكنها ستلبـي قدراً أقل من احتياجات أولئك الذين تحاول مساعدتهم. وقد ينجح بعضها، لكن معظمها سيفشل نظراً لافتقارها إلى الشبكات وإلى المعرفة العميقة وإلى المهارات العملياتية المتوفرة لدى المنظمات المحترفة.

سيؤدي هذا التفاوت بين التسويق الذي تمارسه المنظمات الناشئة وبين ما تنجزه فعلاً إلى إثارة حنق اللاعبين القدماء. عندها، ستتنافس المنظمات غير الحكومية الناشئة مع تلك المؤسساتية على الموارد ذاتها، وستستغل تلك الناشئة معارفها، وحذاقتها الرقمية، ومعرفتها بشرائح مختلفة من جماهير الشبكة لصالحها لتسحب الموارد من المنظمات الأقدم. إذ ستصور المنظمات المؤسساتية الكبيرة

على أنها منظمات متثاقلة غير فاعلة ومنفصلة عن الواقع، ذات نفقات عامة مرتفعة، وكوادر ضخمة لا تتمتع باللمسة الشخصية. وستعد بالمقابل بتقريب المتبرعين أكثر من متلقي الإغاثة بالاستغناء عن الوسطاء، وسيجد المتبرعون المحتملون الجدد المتطلعون للمساعدة في هذا التعهد بالعلاقة المباشرة نقطة جذابة على نحوٍ خاص في عملية البيع بما أن إمكانيات الاتصال تضمن للكثيرين منهم أن يشعروا بأنهم منخرطون شخصياً في الأزمة بالفعل.

لن يكتفي الاختصاصي الشاب في سياتل، الذي لديه الاهتمام ويتحلى بالإيثار وادخر بضعة دولارات، كل كارثة قادمة، بل ستمطر رأسه أفكار عن طرائق للمساعدة، وسيطفح صندوق الوارد لديه ومدخلات تويتر وحساب الفيسبوك ونتائج البحث. وربما غلبه السيل، لكنه سرعان ما سيمشط الخيارات المتاحة أمامه، ويحاول الوصول إلى قرار سريع وجاد، بناءً على ما يراه: أية مجموعة لديها أجمل مواقع الوب شكلاً، وأقوى حضور على الوسائط الاجتماعية، وأبرز الداعمين. كيف له أن يقرر ما هي المنظمة الصحيحة ليتبرع لها، وهو الذي تعوزه الخبرة؟ سيكون عليه الاعتماد على الثقة التي تبعثها لديه مجموعة معينة، وبذلك سيكون قصب السبق من نصيب المنظمات ذات المهارات التسويقية الأكثر قدرة على التأثير فيه (أو في حسابه الافتراضي) مباشرة.

ثمة خطر حقيقي يتمثل في تعرض المنظمات غير الحكومية التقليدية للمزاحمة من قبل هذه المنظمات الناشئة التي سيكون بعضها صادقاً في المساعدة، لكن بعضها الآخر لن يكون كذلك. فالانتهازيون سيستغلون الإمكانيات الجديدة للتسويق المباشر وانحسار عوائق الدخول إلى السوق. وعندما تخضع هذه المجموعات للمحاسبة ستضعف ثقة المتبرعين (وربما تنتج حافزاً لفضح المزيد من المشاركين المحتالين). وسيكون هناك فيض من المشاريع الاحتيالية التي يقف وراءها مشاهير معروفون ورجال أعمال كبار لن تفيد حملاتهم عالية الشحنة سوى في صرف الانتباه عن العمل الحقيقي الذي يجب إنجازه على الأرض. بالإجمال، سيؤدي تحويل إلى منافسة تسويقية إلى ظهور المزيد من اللاعبين، مع تقديم قدر أقل من المساعدة الحقيقية بعد أن تكون المنظمات العريقة قد نحّيت جانباً.

يتطلب التدخل خبرة، كما ذكرنا سابقاً. ففي ميدان أصبح أكثر اكتظاظاً، سيكون من الصعب تنسيق عمليات الإغاثة وتمكين الحكومة من الإشراف ورسم آمال واقعية. ومن شأن التقانة أن تساعد في هذا المجال، حيث يمكن للحكومة الاحتفاظ بقاعدة بيانات مركزية تضم جميع المنظمات غير الحكومية الفاعلة ليجري بعدها تسجيل كل واحدة منها ومراقبتها وتصنيفها في مراتب على منصة شبكية بمساعدة الجماهير. وثمة بالفعل نظم مراقبة وتصنيف للمنظمات غير الحكومية (مثل تشاريتي نافيغيتر، وقاعدة بيانات منظمات المجتمع المدني لدى ون وورلد تراست)، لكنها في معظمها عبارة عن منظمات غير حكومية بدورها. فحتى إذا كانت تساعد في فرض نوع من المحاسبة، وبعيداً عن أنها تسلط الضوء على الممارسات السيئة، فإنها لا تتمتع بأية قدرة على التنفيذ. فتخيل نظام تصنيف ما للمنظمات غير الحكومية تستخدم فيه بيانات حول المنظمات وناشطيها وتمويلها

وإدارتها، إضافة إلى تعقيبات متلقي المساعدات في الأوساط المحلية لتصنيف هذه المنظمات بما يساعد في إرشاد المتبرعين وتوجيه استثماراتهم. سيكون لهذه التصنيفات أثرها في العالم الحقيقي، فقد تؤدي إلى فقدان المنظمات غير الحكومية أهليتها لتلقي التمويل الحكومي إذا انحدر مجموع نقاطها تحت مستوى معين، أو قد تواجه تدقيقاً حكومياً وإجراءات إضافية. وفي غياب نظام تقييم ومراقبة شفاف ومتكامل، ستغرق الحكومات، وكذلك المتبرعون، في سيل من الإغراءات التي تقدمها منظمات الإغاثة، وستكون الوسائل المتاحة لها لتبين المنظمات الصالحة وذات الكفاءة محدودة.

في النهاية، سينتهي الأمر بهذه الفقاعة إلى الانفجار؛ مع تأخر العمليات، وفقدان المانحين المؤسساتيين ثقتهم في مشاريع إعادة الإعمار. وعندما ينقشع الغبار، لن تبقى من هذه المنظمات سوى تلك التي تتمتع بموقعها الصحيح، والتي تركز على أهدافها وتتمتع بولاءٍ قوي من المتبرعين، ولديها تاريخ من العمليات الفعالة والشفافة تتباهى به. وسيكون بعضها مجموعات إغاثة عريقة، بينما سيكون البعض الآخر مجموعات جديدة، لكنها جميعها ستحمل سمات مشتركة معينة تجعلها أصلح لتولي مهام إعادة الإعمار في العصر الرقمي. فهي ستتبع برامج متماسكة تخرج بنتائج غنية بالبيانات، وتدعم جهودها الميدانية بتسويقٍ رقمي حاذق يستعرض عملها ويسمح في الوقت نفسه بتلقي المعلومات الراجعة من المانحين ومن متلقي الإغاثة في آنٍ معاً. وستكون لمظهر قابلية المحاسبة والشفافية أهمية بالغة.

سيستمر أيضاً التوجه نحو المزيد من الارتباط المباشر بين المتبرعين والمتلقين على الأرض. وستعتمد المنظمات غير الحكومية وسائل جديدة تطمح إلى إرضاء هذه الرغبة في تقديم علاقات أكثر حميمية، وهي بذلك ستسرع توجهاً آخر طويل المدى يمكن ملاحظته اليوم، وهو لا مركزية توزيع المساعدات. ونقصد بذلك التخلي عن النموذج المكون من بضعة عقد أساسية (أي مجموعة من المنظمات غير الحكومية المؤسساتية الكبيرة) لتحل محله شبكات من القنوات الصغرى. فبدلاً من التبرع للمكتب الأساسي للصليب الأحمر أو لمنظمة ، سيسعى المتبرعون الذين يزدادون اطلاعاً واستعداداً للمشاركة إلى برامج خاصة محددة تخاطبهم مباشرةً، أو قد يوجهون تبرعاتهم إلى منظمات غير حكومية ناشئة أصغر حجماً تَعِد بتقديم خدمات مكافئة. وستقوم منظمات غير حكومية عريقة تتمتع بالذكاء بدورها بإجراء عملية إعادة صياغة بارعة، حيث تلعب دور المجمّع بعيداً عن البنية الهرمية السابقة، فتعيد اختراع وظيفتها لتتمثل في ربط المتبرعين بالناس الذين يمولونهم مباشرة (موفرةً الشخصية الصحيحة؛ كالربط بين أطباء في بلد متطور مع زملاء لهم في بلد خارج من زلزال)؛ مع الإبقاء على تحكمها المبرمج الكامل (لن يسعى جميع المتبرعين بالطبع إلى التعرف عن قرب بالمنظمات التي يدعمونها؛ وكذلك بالأفراد، وسيكون لدى هؤلاء الخيار بالخروج من مثل هذه المشاركة بسهولة).

ليس لنا أن نهمل الدور الذي يلعبه الأفراد في البلدان التي تعاني من الكوارث أو النـزاعات في بيئة الإغاثة الرقمية الجديدة، فالاتصالات ستؤثر على طريقة

التعامل مع إحدى المشكلات الكبرى التي تواجهها مجتمعات ما بعد الأزمة وأكثرها شيوعاً؛ وهي مشكلة النازحين داخلياً. فليس في وسع الأطراف الخارجية أن تقوم بالكثير لمنع الظروف التي تقود إلى نـزوح داخلي ضمن البلد (كالحرب والمجاعة والكوارث الطبيعية)، لكن الهواتف النقالة ستغير مستقبل الضحايا؛ حيث سيكون معظم النازحين من حاملي هذه الأجهزة، وإذا لم تتوفر لديهم (أو كانوا قد اضطروا إلى تركها وراءهم)، فستقوم مؤسسات منظمات الإغاثة بتوزيع هواتف عليهم، وستُزوَّد مخيمات اللاجئين بنقاط ساخنة لخدمة الجيل الرابع، والتي تسمح للمتصلين بالتواصل في ما بينهم بسهولة ومن دون تكاليف عالية. وبوجود الهواتف النقالة سيصبح تسجيل النازحين أسهل من أي وقت مضى.

يقول معظم النازحين واللاجئين إن أحد أكبر التحديات التي يواجهونها هو نقص المعلومات؛ فهم لا يعلمون أبداً إلى متى سيبقون في مكان معين، أو متى يصل الطعام، أو كيف سيحصلون عليه، أو أين يمكنهم العثور على الحطب والماء والخدمات الصحية، وما هي التهديدات الأمنية التي عليهم الحذر منها. لكن من خلال التسجيل، وباستخدام منصات متخصصة تعالج هذه الأمور، سيتمكن النازحون من تلقي إنذارات تساعدهم على التنقل في بيئتهم الجديدة، وعلى تلقي المؤن والخدمات من منظمات الإغاثة الدولية في مواقعهم. وسيتم استخدام تقنيات التعرف على الوجوه بكثافة لإيجاد الأشخاص الضائعين أو المفقودين. وباستخدام تقانة التعرف على الكلام، يمكن للأميين أن ينطقوا أسماء أقاربهم فتعطيهم قاعدة البيانات جواباً عما إذا كانوا موجودين ضمن نظام المخيم. وستسمح المنصات الشبكية والهواتف النقالة لمخيمات اللاجئين بتنظيم المقيمين فيها وتصنيفهم وفقاً لمهاراتهم وخلفياتهم واهتماماتهم. ففي مخيمات اللاجئين اليوم، ثمة عدد كبير من الناس الذين يتمتعون بمهارات هامة ومطلوبة (من أطباء، ومدرسين، ومدربـي كرة قدم)، ولا يمكن تفعيل مشاركتهم اليوم سوى بطريقة ارتجالية تنتقل ببطء من خلال شبكات شفاهية عبر المخيمات. لذا، يجب أن يتاح للنازحين في المستقبل تطبيق لتتبع المهارات يمكنهم من خلاله التصريح عن مهاراتهم أو البحث في قاعدة البيانات عن مهارات يحتاجون إليها، حيث لا تُترك مهارة إلا وتستغل، ولا يستثنى متطوع من المشاركة.

سيتيح الانتشار الواسع للهواتف المحمولة إمكانيات جديدة أمام المتطلعين إلى تغيير النموذج القائم حالياً لعمليات توزيع الإغاثة. إذ سيكون بإمكان بضعة أفراد جريئين ويتمتعون ببعض المعارف التقنية بناء منصة مفتوحة، يمكن عبرها لمشاركين محتملين في عملية الإغاثة - على غرارهم - أن يدرجوا حاجاتهم ومعلوماتهم الشخصية ويرسلوها إلى السحابة، ثم ينتظروا قدوم أفراد متبرعين يختارونهم ويرسلون المساعدة إليهم مباشرة. ولا يختلف ذلك عن المنصة التي تستخدمها كيفا لتأمين التمويل للمشاريع الصغرية؛ في ما عدا أنه سيكون على نطاق أوسع وذا طبيعة أكثر شخصية، كما سيركز على التبرعات بدلاً من التركيز على القروض (من الطبيعي أن تواجه منصة كهذه سلسلةً من المسائل التخطيطية والقانونية التي سيتوجب عليها معالجتها قبل أن يتاح لها أن تعمل بشكل صحيح).

تخيل الآن أن تعقد هذه المنصة شراكة مع منظمة أكبر منها تستطيع الترويج لها بين جمهور أعرض بكثير في أنحاء العالم، وتؤمن لها معايير تحَقّق معينة تتكفل بطمأنة المستخدمين المتشككين. ففي الغرب، ستقوم أمٌ بأخذ استراحة في أثناء مشاهدة ابنها مباراة كرة قدم، وستتصفح خريطة عالمية حية (تفاعلية ويتم تحديثها لحظياً) على جهاز الآي.باد تبيّن لها من يحتاج إلى شيء ما، وما هو هذا الشيء، وأين يحتاج إليه. وسيكون بمقدورها أن تحدد بالتفصيل من يتلقى تبرعاتها بناء على قصص الأفراد أو مدى حاجتهم وفقاً لتقديرها. وباستخدام نظم تحويل الأموال النقالة المتوفرة سلفاً، تستطيع الأم تحويل المال أو الرصيد النقال إلى المتلقين مباشرة، وبسرعة عفوية؛ كما لو كانت ترسل رسالة نصية.

أما التحدي الذي يفرضه هذا النوع من المنصات فيتمثل في أن عبء التسويق يقع على عاتق متلقي الإغاثة مباشرةً. والحياة في مخيم اللاجئين قاسية بما يكفي، ولا ينقص المرء فيها بعد أن يفكر في ما إذا كان حسابه الشبكي يعبر عن حاجته بطريقةٍ ملائمة أم لا. والمنافسة القوية التي ستنتجها مثل هذه المنصة بين المشاركين على الموارد ستكون مقيتةً بحدّ ذاتها. وثمة أيضاً مخاطرة أن يقوم المتبرعون الذين تعوزهم القدرة على الحكم أو المعرفة بالوضع الميداني بالانحياز في دعمهم لأولئك الذين يقدمون أفضل الحملات التسويقية (أو الذين يتلاعبون بالنظام) بدلاً من دعم أولئك الذين هم في أمس الحاجة فعلاً. فنتيجة الالتفاف على منظمات الإغاثة العريقة، ستفقد هذه المجموعات قدرتها على تبين مستويات الحاجة، وعلى توزيع مواردها توزيعاً مناسباً. وفي غياب مثل هذه الضوابط، ستؤدي هذه التبرعات المباشرة المتاحة للجميع على نحو شبه أكيد إلى توزيع أقل عدلاً لهذه الموارد. فقد أفاد تحليل للإقراض المباشر عبر موقع كيفا أجراه باحثون في سنغافورة بأن المقرضين كانوا يميلون إلى التمييز لصالح المقترضين الأكثر جاذبية والأفتح بشرةً والأنحف.

علاوةً على ما سبق، إن ظهور منظمات كهذه يعني أن هناك افتراضاً بوجود رغبة متبادلة بعلاقة قريبة، وسيكون على متلقي المساعدات أن ينخرطوا طوعاً في هذه العلاقة؛ الأمر الذي قد يصدم كثيرين ممن عملوا في ميدان التنمية كغير مبتدئين. لا شك في أن بعض الناس في بلدان ما بعد الأزمات (وفي البلدان النامية أيضاً) قد يغتنمون الفرصة لتسويق أنفسهم مباشرةً؛ إذا كان ذلك يعني توفر مصدر أكثر موثوقية للتمويل، لكن غالبيتهم لن يكونوا كذلك. فعلى خلاف ما يحدث مع كيفا التي يطلب المشاركون فيها قروضاً، سيكون على هؤلاء أن يطلبوا صدقات على الملأ. والأنفة سمةٌ إنسانية عامة، وغالباً ما يوليها الناس قيمتها الكبرى عندما لا يكون لديهم الكثير غيرها. فمن الصعب تخيل اللاجئين والنازحين وغيرهم من متلقي المساعدات - حتى إذا توفرت لهم منصة تمويل مفتوحة كهذه - يعلنون عن حاجاتهم أمام جمهور عالمي. فمن أهم الوظائف التي تقوم بها منظمات الإغاثة العريقة الحفاظ على المسافة بين المتلقين ومتبرعيهم. لذا، وفي غمرة هذه التغييرات التي أتينا على ذكرها في ما سبق (من منظمات غير حكومية ناشئة، وبرامج تمويل صغري هادفة، ومساعدة غير مركزية)، لا ضير في تذكر الأسباب التي تجعل بعض

الجوانب في عالم التنمية والإغاثة على ما هي عليه، وتسمح لها بتلبية الغرض منها.

فسحة للإبداع

إذا كان من خير في دمار المؤسسات والنظم بعد انقلاب مفاجئ، فهو أن ذلك يفتح الطريق أمام الأفكار الجديدة. والإبداع يتواجد في كل مكان، حتى في الأعمال المجهدة والمعقدة لإعادة الإعمار، وهو سيتحسن بفضل توفر شبكة سريعة وقيادة جيدة وأجهزة أكثر وفرة؛ أي الهواتف الذكية والحواسب اللوحية.

إننا نرى منذ اليوم كيف يتم تعديل أدوات الإنترنت لتلبـي متطلبات بيئة ما بعد الأزمة. وقد قدمت أوشاهيدي (والاسم يعني الشهادة باللغة السواحيلية) - وهي منصة مفتوحة المصدر لتخطيط الأزمات تقوم بجمع البيانات عبر التعهيد الجماهيري لبناء خريطة معلومات حية - مثالاً هاماً على ذلك بعد زلزال هاييتي عام 201. فباستخدام منصة الخرائط البسيطة هذه، قام متطوعو أوشاهيدي في الولايات المتحدة ببناء خريطة أزمة حية خلال ساعة واحدة فقط بعد أن ضرب الزلزال، وخصصوا رمزاً قصيراً (هو 4636) يمكن للناس من خلاله إرسال رسائل المعلومات النصية من مكان الكارثة. وتم الإعلان عنه في ما بعد في محطات الراديو الوطنية والمحلية في هاييتي، وقام مهندسون خارج هاييتي بإضافة البيانات التي تم جمعها إلى خريطة تفاعلية على الشبكة تقوم بتجميع تقارير عن الدمار الحاصل، والمؤن اللازمة، والمحاصرين، وحالات العنف والجريمة. وكانت الكثير من الرسائل النصية باللغة الكريولية، فقامت منصة أوشاهيدي بالتعاون مع شبكة من الآلاف من الهاييتيين الأمريكيين بترجمة المعلومات؛ مما خفض زمن الترجمة إلى عشر دقائق فقط. وخلال بضعة أسابيع كانوا قد قاموا بوضع نحو 2500 تقرير على الخريطة. تقول كارول ووترس مديرة أوشاهيدي في هاييتي للاتصالات والشراكة إن كثيراً من هذه الرسائل كانت تقول فقط "أنا مدفون تحت الأنقاض لكنني لا أزال حياً".

أدت سرعة التفكير وسرعة الترميز لدى أوشاهيدي إلى إنقاذ حياة الناس. وستصبح خرائط الأزمات المشابهة في المستقبل معياراً قياسياً، وسيتم إنشاؤها على الأرجح بقيادة الحكومة. ومن الممكن تجنب بعض المشكلات التي واجهتها أوشاهيدي (كعدم معرفة المنظمات غير الحكومية الأخرى بالمنصة) عبر مركزة البيانات في مصدر رسمي موثوق. وثمة بالطبع خطر وقوع المشروع المقود من قبل الحكومة ضحية البيروقراطية والتشريعات القانونية التي ستمنعه من مواكبة مشاريع غير حكومية مثل أوشاهيدي، لكن إذا كانت الاستجابة فورية، فثمة إمكانية هائلة لأن تتنامى خريطة أزمات تقودها الحكومة حيث تشتمل على معلومات طوارئ أكثر بكثير. ويمكن أن تبقى الخريطة نشطة خلال عملية إعادة الإعمار حيث تصبح منصة تقوم الحكومة من خلالها بمشاركة المعلومات المتعلقة بمختلف مشاريع إعادة الإعمار والبيئات التي تديرها، وتلقيها.

في أي مجتمع خارج من أزمة يمكن إعلام المواطنين بالمناطق الآمنة في أحيائهم (أي الخالية من الألغام أو الميليشيات على سبيل المثال) أو أفضل المناطق من حيث التغطية الهاتفية، أو المواقع الأكثر استثماراً ضمن مشاريع إعادة الإعمار.

وستبقى الحكومة على اطلاع بفضل إبلاغ المواطنين عن حوادث الجريمة أو العنف أو الفساد. ومن شأن نظام متكامل لمعلومات الأزمة ليس فقط منح الشعب مزيداً من الأمان والصحة والاطلاع، بل والتخفيف من الهدر والفساد والتكرار التي غالباً ما ترافق مشاريع إعادة الإعمار. ولن تكون جميع حكومات ما بعد الأزمة مهتمة بتحقيق هذا القدر من الشفافية بالطبع، لكن إذا كان الشعب والمجتمع الدولي مدركين لهذا النموذج على نطاقٍ واسع، فقد يتوفر الضغط الشعبـي الكافي لاعتماده على أية حال. ويمكن الاعتماد عليه في توزيع المساعدة الأجنبية أيضاً. وما من شك في أن الكثير من الشركاء غير الحكوميين سيكونون مستعدين للمشاركة في هذه العملية بالإضافة إلى المتطوعين.

لكن، تكون الأولوية القصوى عادةً لدى دولة خارجة من الأزمة هي إدارة البيئة الأمنية الهشة. ومن شأن الخرائط التفاعلية أن تساعد في هذا المجال، لكنها لن تكون كافية. فاللحظات الأولى التي تلي انتهاء نـزاع ما هي الأكثر حساسية؛ لأنها تفرض على الحكومة المؤقتة أن تبيّن قدرتها على السيطرة والاستجابة، وإلا فإنها تغامر بالتعرض للملاحقة من قبل الشعب الذي نصبها بالذات. ولكي تستمر الحياة اليومية، لا بد للمواطنين من أن يشعروا بما يكفي من الأمان لإعادة افتتاح أعمالهم وإعادة بناء منازلهم وإعادة زرع محاصيلهم. والتخفيف من التوتر في البيئة أمر حاسم لبناء ثقة المواطنين خلال عملية إعادة الإعمار. ومن شأن الاستخدامات المتبصرة للتقانة أن تساعد الدولة على تأكيد حكم القانون بطرق لا يستهان بها.

ستصبح الهواتف النقالة - بفضل الوظائف التي تقدمها - قنوات أساسية، وممتلكات قيمة، حين تعمل الدولة على معالجة البيئة الأمنية. ففي البلدان التي تستطيع جيوشها القيام بدورها، يعتمد دعم الناس لحكم القانون (كنقيض للانشقاق وارتكاب الجرائم أو الاستيلاء على السلطة) على ثقتهم بكفاءة الحكومة أكثر مما يعتمد على خصال شخصية. وإذا أردنا التبسيط، فإن كل ما يهم معظم أولئك الذين يرتدون بذلة هو ما إذا كانوا سيتلقون شيكاً بالراتب بشكل موثوق ومن دون أن يتعرضوا إلى استغلال كبير، وهم بحاجة إلى معرفة المسؤول عن ذلك.

ستساعد المنصات التقانية في المستقبل على فرض القانون في إطار هذه العملية عبر تزويد كل ضابط شرطة أو جيش بجهاز خاص يحتوي على العديد من التطبيقات المتميزة (وعالية الأمان). فسيتولى أحد التطبيقات إدارة الرواتب ليلعب دور الواجهة بين الضباط ووزارتهم التي تدفع لهم. وقد أطلقت شركة روشان للاتصالات في أفغانستان برنامجاً تجريبياً لتسديد رواتب ضباط الشرطة الوطنية الأفغانية إلكترونياً عبر منصات الصيرفة النقالة في خطوة جريئة تهدف إلى إنهاء الفساد المستشري الذي يشل الموارد المالية للبلاد. وعلى هذه الهواتف المخصصة، قد يطلب تطبيق آخر من الضباط كتابة تقارير عن نشاطاتهم اليومية - كما يفعلون في سجل الأداء - ليخزنوا هذه المعلومات على السحابة، حيث يستطيع قادتهم التنقيب فيها والخروج بمقاييس لقياس مدى الفعالية والتأثير. ويمكن لتطبيقات أخرى أن تقدم نصائح تدريبية أو مستشارين افتراضيين للضباط الملتحقين حديثاً (كما حدث في ليبيا عندما تم دُمج الكثير من مقاتلي الميليشيات

في الجيش المحدث). ويمكنها تأمين فضاءات افتراضية على الشبكة للإعلام عن حالات الفساد وغيرها من النشاطات غير الشرعية من قبل الضباط الآخرين من دون الكشف عن هوية المُبَلِّغ.

من شأن تقارير المواطنين الواردة عبر منصات نقالة أن تزيد من قدرة الدولة على الحفاظ على الأمن إذا اختار الطرفان أن يعملا معاً. فكل مواطن يحمل هاتفاً نقالاً قد يتحول إلى شاهد ومحقق. وهؤلاء المواطنون أكثر توزعاً من أية هيئة تنفيذية، وهم مستعدون لتوثيق الاعتداءات التي يشهدونها. وفي أفضل الحالات، سيختار المواطنون المشاركة في مهام الحراسة النقالة هذه، سواء أكانت مشاركتهم بدافع الشعور الوطني أم نتيجة اهتمام شخصي. وسيساعدون، يداً بيد مع الدولة، على بناء مجتمع أكثر أمناً ونـزاهة. أما في أسوأ الحالات، فستفقد شرائح عريضة من الشعب ثقتها بالحكومة، أو قد تفضل المقاتلين السابقين (كأولئك الذين خاضوا المعركة ضد القذافي). وقد يتم استخدام قنوات تقارير المواطنين هذه لمشاركة معلومات مزيفة وإضاعة وقت الشرطة.

ستكون مشاركة المواطنين عاملاً حاسماً في المسائل الأمنية الأولية أيضاً. فباستخدام المنصات الصحيحة، وبتوفر ميل الحكومة إلى الشفافية، قد يتمكن الناس على الأرض من مراقبة التقدم المحقق، والإعلام عن حالات الفساد، ومشاركة الاقتراحات، بما يجعلهم جزءاً من المحادثات الجارية بين الحكومة والمنظمات غير الحكومية والفاعلين الأجانب. وسيستخدم الجميع الهواتف النقالة، فقد تحدثنا مع الرئيس الرواندي باول كاغام، الذي يبقى من بين القادة الأكثر معرفة بالتقانة في أفريقيا، وسألناه عن أثر التقانة النقالة في تغيير طريقة تعامل المواطنين مع التحديات المحلية، فرد قائلاً: "حين يحتاج الناس إلى شيء، سواء أكان اقتصادياً أم أمنياً أم اجتماعياً، فإنهم يلجأون إلى هواتفهم. فهي الطريقة الوحيدة التي يحمون بها أنفسهم. وأولئك الذين يحتاجون إلى مساعدة فورية، سيتلقونها"، وهذا كفيل بتغيير شروط الحياة، بالنسبة إلى شعوب البلدان النامية - يشرح لنا - وخصوصاً تلك الخارجة لتوها من نـزاع أو أزمة. فبناء الثقة بالحكومة مهمة حاسمة، ويمكن تسريع هذه العملية وجعلها أكثر ديمومة عبر زيادة مشاركة الناس من خلال المنصات المفتوحة: "وضعنا في رواندا برنامجاً يقوم المواطنون فيه بتمرير المعلومات"، يقول كاغام، مشدداً على أن استخدام التقانة جعل البرنامج أكثر فعالية بكثير.

مع تحول التعهيد الجماهيري إلى ميزة ملازمة لعملية فرض القانون في المستقبل (على الأقل في مرحلة ما بعد النـزاع أو الكارِثة) ستنشأ ببطء ثقافة المحاسبة. سيبقى الخوف من السلب والعنف قائماً، لكن المجتمعات في المستقبل ستكون قد وثَّقت جميع ممتلكاتها الشخصية وآثارها التاريخية على الشبكة؛ حيث يتم التعرف على المفقودات مباشرة عند استعادة الأمن. وسيكافَأ المواطنون على إرسالهم صوراً للصوص (حتى إذا كانوا من الشرطة) تُبيِّن وجوههم وغنائمهم. وسيبقى خطر الانتقام قائماً، لكن ثمة أدلة تبيّن أنه بالرغم من خوف الناس، يبقى هناك - دائماً تقريباً - عدد كبير منهم مستعدّ لتحمل هذه المجازفة.

وكلما كثر أولئك المستعدون للإبلاغ عن جريمة، انخفض مستوى الخطر الذي يهدد الفرد. فتخيل لو حدث نهب متحف بغداد الشهير في العراق عام 2003 بعد عشرين عاماً، فكم من الوقت كان من الممكن لأولئك اللصوص أن يخفوا كنوزهم (ناهيك عن أن يحاولوا بيعها) لو جرى تسجيل السرقة مباشرة ونشرها في أنحاء البلاد وتوفرت للمواطنين الآخرين دوافع كافية للإبلاغ عنهم؟

يلحق ضياع الآثار الضرر بكرامة أفراد المجتمع، ويمنعهم من الحفاظ على ثقافتهم. لكن الأسلحة الضائعة تمثل خطراً أكبر بكثير على استقرار البلاد. فعادةً، تختفي الذخائر والأسلحة الصغيرة بعد النـزاعات وتجد طريقها إلى السوق السوداء (التي تقدر قيمتها بمليار دولار سنوياً)، لتظهر في ما بعد في أيدي المليشيات والعصابات والجيوش في بلدان أخرى، وقد تمثل شرائح معرف التردد الراديوي حلاً لهذه المشكلة. فهذه الشرائح أو الرقع تحتوي على معلومات مخزنة إلكترونياً، ويمكن تصنيعها بحجم حبة الأرز، وهي موجودة في كل مكان اليوم، وفي كل شيء؛ بدءاً من هواتفنا وجوازات سفرنا إلى المنتجات التي نشتريها (بل إنها موجودة حتى في حيواناتنا الأليفة، فثمة شرائح تزرع تحت الجلد أو تثبت على الأذن، وتستخدم للمساعدة على التعرف على الحيوانات الضائعة). وإذا وقّعت الدول الكبرى على معاهدات تفرض على مصنعي الأسلحة زرع شرائح تردد راديوي غير قابلة للإزالة في جميع منتجاتها، فسيجعل ذلك عملية البحث عن مخابئ الأسلحة وحظر شحنها أسهل بكثير. ونظراً لقابلية شرائح اليوم إلى التدمير بواسطة الميكرووايف، فإن الشرائح في المستقبل ستحتاج إلى وقاء يحميها من العبث (ونحن نفترض أن لعبة قط وفأر تقنية ستجري بين الحكومات الساعية لتتبع الأسلحة ذات شرائح معرف التردد الراديوي وتجار الأسلحة الذين يريدون التعامل بالأسلحة من تحت الطاولة). وعندما تضبط أسلحة تحمل هذه الشرائح، سيكون من الممكن تعقب الأمكنة التي كانت فيها إذا كانت الشرائح نفسها مصممة بطريقة تخزن فيها بيانات الموقع. وإذا كان ذلك لا يكفي لإيقاف الاتجار بالأسلحة، فإنه سيضغط على اللاعبين الكبار في هذه تجارة.

كثيراً ما ترغب الدول التي تتبرع بالأسلحة للحركات الثورية بمعرفة ما يحدث لهذه الأسلحة. ومع رقائق المعرف الراديوي يمكن تتبع مثل هذه الاستثمارات، فالثوار الليبيون كانوا مجموعة غير معروفة بالنسبة إلى الجميع تقريباً، وبغياب إمكانية التعقب، كان على الحكومات التي توزع الأسلحة عليهم أن توازن بين مكسب نجاح الثورة وبين العقبات المحتملة كأن تنتهي هذه الأسلحة في سراديب سرية (في بداية عام 2012، ظهرت بعض الأسلحة التي كانت الميليشيات الليبية تستخدمها في مالي بين أيدي مقاتلي الطوارق الساخطين. وأدى ذلك، مع عودة سرية الطوارق التي حاربت مع جيش القذافي، إلى حملة عنيفة ضد الحكومة وفرت شروط انقلاب عسكري).

لتحقيق توزيع الأسلحة على نحو قابل للتعقب إلكترونياً، لا بد من التغلب على العقبات التي تقف في طريقه. فهو يكلف المال لتصميم الأسلحة التي تتضمن شرائح معرفات التردد الراديوي. ومصنعو الأسلحة يتربحون من سوق غير شرعية

ضخمة يبيعون فيها منتجاتهم، كما أن الدول - وتجار الأسلحة - تستطيب توزيع الأسلحة على نحو مغفل الهوية؛ كما هي الحال اليوم. فمن الصعب تخيل قوةٍ عظمى تضحي طوعاً بقدرتها على إنكار مسؤوليتها - بطريقةٍ لا بد للآخرين من تصديقها - عن مخابئ الأسلحة والأسلحة الموزعة سراً، مقابل خيرٍ أعظم طويل الأمد. علاوةً على ذلك، قد تدعي الدول أن زرع أسلحة بلد آخر على نحو مزيف في منطقة صراع قد يشير إلى تورطها؛ مما يؤدي إلى تفاقم النـزاع أكثر بعد، لكن الضغط الدولي قد يحدث فرقاً.

لحسن الحظ، إن هناك الكثير من الطرق التي يمكن من خلالها استخدام تقانة المعرفات الراديوية على المدى القصير خلال مشاريع إعادة الإعمار. إذ يمكن أن تستخدم شارات المعرفات الراديوية لتتبع عمليات توزيع الإغاثة والمؤن الأساسية الأخرى، والتأكد من شرعية المستحضرات الصيدلية وغيرها من المنتجات، والحد بشكل عام من الهدر والاستغلال في مشاريع التعهدات الكبرى. وقد قام برنامج الغذاء العالمي بتجارب خلال توزيع الأغذية في الصومال باستخدام الشيفرات الخيطية ورقاقات المعرفات الراديوية لتحديد الموزعين النـزيهين الذين يقومون بإيصال الأغذية إلى المناطق الهدف فعلاً. وبإمكان نظام تعقب (غير مكلف وشامل وموثوق) كهذا أن يساعد مساعدة جلية في تنظيم متاهة توزيع المساعدات عبر تحسين إمكانيات المحاسبة، وتأمين البيانات التي يمكن استخدامها لقياس مدى النجاح والفعالية؛ حتى في الأماكن الأقل غنى بالاتصالات.

ثمة استخدام مبتكر آخر للأجهزة النقالة أمام حكومات ما بعد النـزاع يتعلق بالتعامل مع المقاتلين السابقين. فمقايضة الأسلحة بالأجهزة قد يصبح أحد المقومات الأساسية لبرنامج نـزع السلاح والتسريح وإعادة الدمج (دي.دي.أر). وقد أشرفت حكومة باول كاغام - على الرغم من الجدل الذي تثيره في مجال حقوق الإنسان وحكم الأقليات - بالإشراف على عمليات نـزع السلاح لعشرات الآلاف من المقاتلين السابقين في إطار مشروع التسريح وإعادة الدمج الرواندي. "نعتقد أن علينا أن نضع بين أيدي المقاتلين السابقين أدوات يغيرون بها حياتهم" يشرح لنا. وضمن الحزم التي يتم تسليمها لهؤلاء المقاتلين السابقين "نعطيهم بعض المال، لكننا نعطيهم أيضاً هواتف لكي يروا الإمكانيات المتوفرة". كما يتلقى معظم المقاتلين السابقين الذين يمرون بالبرنامج - الذي لا يزال جارياً في رواندا - نوعاً من التدريب يحضرهم لإعادة الاندماج في المجتمع. وتمثل المعالجة النفسية مكوناً مهماً أيضاً. وقد رأينا هذه البرامج في أثناء تنفيذها، فهي أشبه بالمعسكرات الصيفية، لما تضمه من قاعات دراسية ومهاجع ونشاطات. وهي مناسبة هنا؛ بما أن عدداً كبيراً جداً من المقاتلين السابقين في رواندا من الأطفال عملياً، والأساس هنا هو منحهم انطلاقة جديدة بصحبة المئات غيرهم ممن لديهم تجارب مشتركة، ثم بناء ثقتهم بوجود حياة جيدة على الطرف الآخر من الصراع.

يشير كلام كاغام إلى أننا لسنا بعيدين عن اللحظة التي ستجرب فيها بلدان أخرى هذا البرنامج. فبعد كل نـزاع، يحتل نـزع سلاح المقاتلين السابقين الأولوية العليا (نـزع السلاح، أو ما يسمى أحياناً اللاعسكرة أو ضبط الأسلحة، هو عملية

نـزع القدرات العسكرية للفصائل المحاربة، سواء أكانت من المتمردين، أم من الأعداء المدنيين، أم من فصائل الجيش المتبقية من النظام السابق)، فضمن برنامج نـزع أسلحة نموذجي، تنتقل الأسلحة من الأطراف المتحاربة إلى قوات حفظ السلام خلال فترة محددة، وغالباً ما يشتمل ذلك على نوعٍ ما من التعويضات. وكلما طال النـزاع، استغرقت هذه العملية وقتاً أطول. فقد احتاجت ولادة دولة جنوب السودان سنواتٍ طويلة من الاقتتال بين الشطرين الشمالي والجنوبـي للبلاد (وقد أتيحت لنا فرصة زيارتها في كانون الثاني عام 2013)، وسرعان ما بات واضحاً بالنسبة إلى حكومة جنوبـي السودان وللمجتمع الدولي أنّ هناك حاجة ماسّة إلى برنامج نـزع سلاح شامل. ومع مساعدات بلغت 380 مليون دولار من الأمم المتحدة والصين واليابان والنرويج والولايات المتحدة، اتفق السودانيون على طرفي الحدود على نـزع سلاح نحو 200 ألف جندي سابق بحلول عام 2017. وتعهد بلدان مجاوران، هما أوغندا وكينيا، أقلقهما احتمال انتشار المحاربين بعد تحولهم إلى مرتزقة إضافة إلى النقل غير المشروع للأسلحة عبر الحدود، بتقديم دعمهما لتعزيز الأمن الإقليمي، وكان ذلك عنصراً حاسماً في الخطة. إلا أن مناطق قليلة في العالم تنافس منطقة البحيرات الكبرى في تقلباتها وفي قابلية اندلاع النـزاعات فيها، لذا يجب أن يتم تناول هذه التعهدات بحذر.

تحتوي معظم بيئات ما بعد النـزاع على مقاتلين سابقين مسلحين يجدون أنفسهم بلا عمل ولا هدف ولا مركز ولا قبول من المجتمع. وإذا بقيت هذه المشكلات من دون علاج فقد تدفع بالمقاتلين السابقين إلى العودة إلى العنف (كمجرمين أو كأفراد في الميليشيات أو كمرتزقة). خصوصاً إذا كانوا لا يزالون محتفظين بأسلحتهم. وعندما تسعى الحكومات إلى منحهم دوافع لتسليم بنادقهم، فقد يجد هؤلاء في الهواتف الذكية أكثر مما يكفي للانطلاق. فالمقاتلون السابقون يحتاجون إلى التعويض وإلى الاعتراف بهم، وإلى خطوة تالية يخطونها. وإذا فهموا أن الهاتف الذكي لا يمثل فقط فرصة للاتصال، بل أيضاً طريقة لتلقي المخصصات والدفعات المالية، فسيصبح الهاتف استثماراً يستحق مقايضته بالسلاح.

سيقدم كل مجتمع حزماً مختلفة قليلاً ضمن مبادرته وفقاً للثقافة ومستوى التقدم التقاني. لكن أساسيات العملية تتمتع بجاذبية عالمية، فهي تشتمل على أجهزة مجانية من أحدث طراز، ومراسلات نصية واتصالات صوتية رخيصة ورصيد لشراء التطبيقات، ودعم بالبيانات يسمح للناس باستخدام الإنترنت والبريد الإلكتروني من دون كلفة كبيرة. وستكون هذه الهواتف الذكية أفضل جودة مما يتوفر لدى الكثير من أفراد الشعب الآخرين، وأرخص استخداماً أيضاً. ويمكن تجهيزها مسبقاً بتطبيقات مهنية جذابة تعطي المقاتلين السابقين بعض الدفع في محاولة صعودهم، مثل تعليم اللغة الإنكليزية، بل وحتى التعليم الأساسي. فيمكن لطفل، كان محارباً سابقاً في جنوب السودان، ويقيم اليوم في مخيم للاجئين بعد أن كان قد أجبر على ترك عائلته في سن صغيرة، أن يستخدم جهازاً يصله ليس فقط بأقاربه المحليين، بل وبمستشارين محتملين من المهاجرين السودانيين في الخارج قد يكون من بينهم شباب نجحوا في الحصول على لجوء في الولايات

المتحدة وقاموا ببناء حياة جديدة تماماً لأنفسهم.

سترغب الدول المانحة غالباً في تولي تكاليف مثل هذا البرنامج في مراحله الأولى لتقوم بعد ذلك بتسليم الأمر - مالياً وإدارياً - إلى الدولة المعنية، مما سيسمح للحكومة بالاحتفاظ ببعض النفوذ على المقاتلين السابقين في مجتمعها. ومن الممكن تجهيز الهواتف ببرمجيات تسمح للدولة بتعقب المقاتلين السابقين، أو بمراقبة سجل تصفحهم لفترة من الزمن، ليبقى المقاتلون السابقون تحت طائلة فقدان رصيد التصفح أو الهاتف نفسه إذا لم يلتزموا بقواعد البرنامج. يمكن للدولة أن تتبع سياسة ثلاثية المراحل وفقاً للبيانات الجغرافية لهذه الهواتف. ففي أول مرة لا يسجل المقاتل السابق فيها دخوله لدى المسؤول عنه الذي يكون بمثابة ضابط التأهيل، في الوقت المحدد، يتلقى تحذيراً قصيراً بالفيديو، وفي المرة الثانية يتم إيقاف رصيد التصفح لديه لبعض الوقت، أما المرة الثالثة فستؤدي إلى إلغاء رصيد التصفح واستعادة الجهاز.

سيكون التنفيذ تحدياً بالطبع، لكن الدولة ستحافظ أقله على قدر من النفوذ أكبر مما كانت ستحققه لو منحت دفعة نقدية لمرة واحدة. وثمة طرق لجعل هذا البرنامج مرغوباً؛ بعيداً عن التطبيقات المفيدة والهواتف التي تدل على منـزلة. فغالباً ما سيعتمد المقاتلون السابقون على الرواتب التقاعدية والمخصصات لتأمين قوت عائلاتهم. لذا، إن دمج هذه الدفعات في نظام مالي نقال سيكون طريقة ذكية لإبقاء المقاتلين السابقين على الصراط المستقيم.

إلا أنه لكي ينجح مشروع السلاح مقابل الهاتف هذا، لا بد من ربطه ببرنامج شامل وناجح. فالهواتف النقالة وحدها لن تستطيع تحقيق اندماج آلاف المقاتلين السابقين بطريقة قابلة للاستمرارية. وكجزء من برامج إعادة الدمج والمحاسبة، قد يتلقى بعض المقاتلين السابقين مالاً أو ميزات خاصة لأجهزتهم لقاء تسليم صور مخابئ أسلحة أو مقابر جماعية. وسيحتاج المقاتلون السابقون إلى الشعور بأنهم قد عوملوا بعدل، وأنه تم تعويضهم على نحو لائق لكي يسلموا أسلحتهم ويتنازلوا عن الشعور بالسلطة الذي تمنحهم إياه في الوقت نفسه. وستلعب البرامج التي تشتمل على تقديم الاستشارات ودروس المهارات المهنية دوراً هاماً في مساعدة هؤلاء الأفراد على التحول إلى الحياة المدنية.

ففي كولومبيا، تم تطبيق برنامج ناجح جداً لنـزع السلاح يهدف إلى إعادة دمج مقاتلي الغوريللا السابقين في المجتمع، ويعتمد على شبكة كبيرة من المراكز التي تقدم لهم خدمات تعليمية وقانونية ونفسية وصحية. وبخلاف الكثير من برامج نـزع السلاح الأخرى التي كانت تدار بعيداً جداً عن مراكز المدن، اتخذت الحكومة الكولومبية خطوة جريئة حين وضعت الكثير من بيوت الإدماج هذه في وسط المدينة. فقد أدركت الحكومة في وقت مبكر ضرورة بناء الثقة بالبرنامج، من طرف المقاتلين السابقين ومن المجتمع على حدّ سواء. وأصبحت هذه البيوت المعدة بطريقة تشبه مآوي المراهقين الهاربين جزءاً من المجتمع، تشرك الجيران وغيرهم من السكان المحليين في عملها. واستخدمت الحكومة هؤلاء المقاتلين السابقين كنماذج تبين لماذا يجب على الكولومبيين عدم اللجوء إلى العنف. فكانوا يتحدثون

في الجامعات، ويخاطبون عناصر سابقين من القوات المسلحة الثورية في كولومبيا (وهي منظمة إرهابية كولومبية عمرها 48 عاماً)، وينظمون طاولات مستديرة محلية.

ليس من الواضح ما إذا كانت تقانات الاتصالات ستساعد في عملية المصالحة بين غير المحاربين أم ستعيقها. إذ سيساعد الانتشار الشامل للأجهزة خلال النـزاع على تمكين المواطنين من جمع أدلة يستخدمونها في طلبهم للعدالة في بيئة ما بعد النـزاع من جهة، لكن من جهة أخرى، ومع تسجيل كل هذا القدر من العنف والمعاناة على وسائط رقمية (تخزيناً أبدياً، وعلى نحو قابل للتداول على نطاق واسع)، من المحتمل أن تترسخ الانقسامات الاجتماعية والإثنية التي أشعلت الصراع حين تخرج كل هذه البيانات إلى العلن. وعملية تعافي المجتمعات التي مزقتها الصراعات الأهلية والإثنية تنطوي على ما يكفي من الألم، وهي تتطلب قدراً معيناً من فقدان الذاكرة الجمعية. ووجود المزيد من الأدلة سيفرض الحاجة إلى قدر أكبر من الغفران.

ستُستخدَم التقانة في المستقبل لتوثيق مختلف عمليات تحقيق العدالة في أثناء تنفيذها وتسجيلها. وتشتمل هذه العمليات على الإصلاح والعلاج (كمشاريع اجتثاث البعث) ومهام المصارحة والمصالحة، بل وحتى المحاكمات. حيث ستجعل التقانة جميع هذه الإجراءات منفتحة وشفافة. ولهذا التحول سلبياته وإيجابياته. فقد كانت المحاكمات المتلفزة لصدام حسين مريحة بالنسبة إلى الكثير من العراقيين، لكنها منحت الديكتاتور السابق وأنصاره مسرحاً يمثلون على خشبته. لكن، مرة أخرى، كما توقع نيجل سنواد، عامل الإغاثة المخضرم لدى الأمم المتحدة سابقاً، والذي يعمل اليوم لدى غوغل، "يمكن لمجموعات حقوق الإنسان ومجموعات القصاص بناء نظام يمكّن الناس من إقامة النصب التذكارية، ومن رواية حكايات أولئك الذين قضوا أو اختفوا خلال النـزاع". وباستخدام مثل هذه الشهادات والنصب التذكارية - كما يقول - يمكن للمجموعات "جمع القصص من الجانبين؛ على الرغم من تضارب الروايات ونشوب حروب اللهب (تراشق بالكلام على الإنترنت عبر قوائم المناقشة والتعليقات) على الشبكة من حين لآخر؛ لتنتج جواً ملائماً للاعتذار والاعتراف بالحقيقة وتحقيق المصالحة".

لن تفيد تقانة الإنترنت في تغيير الآليات البطيئة والمؤلمة لعملية المصالحة، وليس هذا من واجبها. فالاعترافات العلنية بالذنب، والإدانات والعقوبات، ومبادرات الصفح، تلعب جميعها دوراً تطهيرياً في مجتمع يعمل على التعافي من نـزاع. فالنماذج القائمة اليوم من المحاكمات الجنائية على المستوى الدولي (في ما يتعلق بالجرائم ضد الإنسانية) بطيئة وبيروقراطية وعرضة للفساد. ويقبع عشرات المجرمين في المحكمة الجنائية الدولية (التي تدرج تسميتها بمحكمة الهيك أيضاً) شهوراً طويلة لمجرد البدء بمحاكمتهم. وكثيراً ما تُفضَّل نظم المحاكم المحلية والهيئات الأهلية على المؤسسات الدولية المتلكئة في بيئات ما بعد النـزاع اليوم.

من المرجح أن يكرس انتشار التقانة هذا التوجه. إن الكم المتوفر من الأدلة الرقمية المتعلقة بالجرائم والعنف سيرفع الآمال بإمكانية تحقيق العدالة، لكن

الوتيرة الجليدية التي تبديها الهيئات القضائية الدولية، كالمحكمة الجنائية الدولية، ستحد من سرعة تبني هذه الهيئات لهذه التغييرات. فليس من الوارد على سبيل المثال أن تتقبل المحكمة الجنائية الدولية ذات يوم ملفات فيديو غير محققة تم تصويرها باستعمال هاتف نقال كدليل ضمن محاكماتها الإجرائية جداً (مع أن منظمات أخرى مثل ويتنيس تحاول تحدي ذلك). لكن النظم القضائية المحلية التي تتمتع بقدر أقل من القيود القانونية، وبتوجه أكثر مرونة، قد تكون أكثر انفتاحاً على التطورات في مجال العلامات المائية الرقمية التي ستسمح بالتوثق من الفيديوهات الأصلية بطريقة عملية. وسيبدي الناس ميلاً متزايداً لهذه الطرق القضائية.

إن الإطار المحلي يعني أن الحكام، سواء أكانوا قضاة رسميين، أم زعماء قبائل، أم قادة في المجتمع، يتمتعون بالتأكيد بمعرفة واسعة وحميمية بالمجتمع من حيث دينامياته الداخلية، والفاعلين الرئيسين، والأوغاد الكبار فيه، وجميع الأمور الدقيقة التي سيكون على الهيئات الدولية أو الخارجية أن تناضل لاستيعابها. وعندما تقدم إليهم الأدلة الرقمية، ستكون الحاجة إلى التحقق أقل، لأنهم يألفون الناس والأماكن مسبقاً. في ظروف ما بعد الأزمة، سيمارس المجتمع ضغطاً خاصاً لإحقاق العدالة بسرعة. ويبقى طرح موضوع ما إذا كانت هذه المحاكم أكثر أم أقل عدلاً مقارنة بقرينتها الدولية موضوعاً للنقاش، لكنها ستكون بالتأكيد أسرع في حركتها.

قد يتجلى هذا التوجه في المستقبل في لجان المصارحة والمصالحة، أو في بنى قضائية مؤقتة يتم إنشاؤها بعد صراع كبير. فبعد الإبادة الجماعية في رواندا، رفضت الحكومة الجديدة في البلاد نموذج المصارحة والمصالحة جنوب الأفريقي محاججة بأن المصالحة لن تتم إلا إذا عوقب المذنبون. لكن النظام القضائي الرسمي استغرق وقتاً أطول من اللازم لمعالجة قضايا المتهمين بارتكاب المجازر الجماعية. وقبع أكثر من مئة ألف رواندي في السجن لسنوات عدة بانتظار مثولهم أمام المحكمة. ثم تم بناء نظام جديد من المحاكم المحلية المستوحاة من أسلوب لحل النـزاعات اعتماداً على المجتمع وعلى القواعد الشعبية يعرف باسم غاشاشا. وأمام محاكم الغاشاشا كان المتهمون يواجَهون من قبل المجتمع، وتعرض عليهم أحكام بديلة إذا اعترفوا بجرائمهم، أو شرحوا ما حدث، أو دلّوا على بقايا ضحاياهم. وعلى الرغم من كونه نظاماً قضائياً قروياً، إلاّ أنّ لنظام محاكمات الغاشاشا بنية معقدة تشتمل على عدة مراحل تسبق إصدار الحكم. وتسمى المرحلة الأولى مستوى الخلية، حيث يُحضر فيها المتهمون أمام محكمة تتألف من أشخاص من المجتمع الذي ارتكبت فيه الجريمة، ويحدد هؤلاء مدى فظاعة الجريمة، وما إذا كان يجب أن يحاكم المتهمون على مستوى الدائرة أم المقاطعة أم الإقليم، والتي تتعامل كلها بالاستئناف. ونظام الغاشاشا أبعد ما يكون عن الكمال، فهو ينضح بالانحيازات الثقافية التقليدية، كإقصاء النساء من السلك القضائي، والعجز عن ملاحقة الجرائم المرتكبة ضد النساء بالصرامة نفسها التي يتبعها مع تلك المرتكبة بحق الرجال. لكن، بعيداً عن هذه المحاذير، كانت العدالة سريعة، وكان المجتمع المشارك فيها يشعر بالرضا عن المحاكمة بشكل عام. وقد سعت حكومات ما بعد

الأزمة في أنحاء أخرى من العالم في ما بعد إلى تبني هذا النموذج نظراً لفعاليته في تحقيق العديد من أهداف المصالحة.

سواء أختار المواطنون في المستقبل أخذ أدلتهم الرقمية إلى المحكمة الجنائية الدولية أم إلى الهيئات القضائية المحلية، فإنهم بالتأكيد سيحظون بفرص أفضل للمشاركة في عملية العدل والمصالحة الانتقالية. ويمكنهم تحميل الوثائق والصور وغيرها من الأدلة المتعلقة بنـزاع، أو بنظام استبدادي سابق، إلى بنك معلومات دولي في السحابة يقوم بتصنيف المعلومات وإضافتها إلى الملفات المفتوحة ذات الصلة، لتستخدم في ما بعد في المحاكم، ومن قبل الصحفيين وغيرهم. وستساعد النصب التذكارية التشاركية وحلقات التغذية الراجعة الحصرية التي تسمح للناس بالتعبير عن مظالمهم بطريقة منظمة (وقد تستخدم المجتمعات خوارزميات ربط البراهين لتجميع معلومات أكثر إلزاماً) على تعزيز ثقة المجموعات التي قد تشعر بأنها عرضة للإهمال عندما ينفض النـزاع. وسيتمكن المواطنون من مشاهدة العملية القضائية وهي تتكشف أمامهم على هواتفهم بالزمن الحقيقي مع البث الحي لمحاكمات الشخصيات الكبرى في الطرف الآخر من العالم ترافقه ثروة من المعلومات حول كل مرحلة من مراحل المحاكمة. وتوثيق جرائم (سواء أكانت مادية أم افتراضية) لنظام ساقط يلبـي أهدافاً أبعد من مجرد المحاكمة، فعندما تنشر جميع الأسرار القذرة لدولة سابقة على الشبكة، لن تستطيع أية حكومة مستقبلية أن تقوم بالأشياء نفسها تماماً. والمراقبون السياسيون يخشون دائماً أن تنـزلق دولة ما بعد النـزاع وتعود إلى الاستبداد، وهم يراقبون بيقظة بحثاً عن أية علامات تشير إلى مثل هذه العودة. لكن الكشف الكامل عن آثام النظام السابق (أي كيف كان يتعامل بوحشية مع معارضيه، وكيف كان يتجسس على النشاطات الشبكية لمواطنيه، وكيف كان يخفي المال خارج البلاد) سيساعد على منع مثل هذه الاحتمالات.

من بين جميع المواضيع التي قمنا بتغطيتها، قد يكون مستقبل إعادة الإعمار هو الأكثر مدعاةً للتفاؤل. فقليلة هي الأشياء التي يمكن أن تكون مدمرة بالنسبة إلى بلد وشعب أكثر من كارثة طبيعية أو حرب أو كلتيهما معاً. لكننا مع ذلك نرى ميلاً واضحاً لأن تكون تحولات ما بعد الأزمة أسرع وقادرة على تحقيق نتائج أكثر إرضاء. وعلى خلاف الكثير من التوجهات السائدة في علم السياسة الطبيعية، فإن العالم يتعلم بالفعل، من كل مثال جديد لعملية إعادة الإعمار، ما الذي يمكن أن ينجح، وما الذي لا يمكن أن ينجح، وما الذي يمكن تحسينه. وستؤدي التطبيقات الذكية لتقانة الاتصالات والانتشار الواسع لإمكانيات التواصل، إلى تسريع عملية إعادة البناء وزيادة اطلاع الناس وقوتهم. وستساعد على بناء مجتمع أفضل وأقوى وأكثر مرونة. فكل ما يتطلبه ذلك هو بعض الإبداع، والكثير من سعات النقل الشبكية، والاستعداد للابتكار.

خاتمة

عندما نتفكر في المستقبل، بوعوده وتحدياته، نجد أمامنا عالماً جديداً شجاعاً. إنها الحقبة الأسرع وتيرة والأكثر إثارة في التاريخ البشري. وسنشهد المزيد من التغيير بعد، وبمعدل أسرع من أي جيل سبقنا، وسيكون هذا التغيير، المدفوع في جزء منه بالأجهزة التي نحملها بين أيدينا، أكثر فردانية وتشاركية مما يمكننا أن نحيط به بخيالنا.

عام 1999 قدم عالم المستقبليات راي كورتسفايل في كتابه **عصر الآلات الروحية: عندما تتجاوز الحواسب الإنسان في ذكائه**، فيقول: "التقانة استمرارية للتطور [الطبيعي] بطرق أخرى، وهي بحدّ ذاتها عملية ثورية". فالتطور يبني نظامه المتعاظم الخاص، حيث يقود إلى نمو أسي ومعاودات متسارعة مع الزمن. والحسابات - التي تشكل العمود الفقري لكل تقانة نشاهدها اليوم - تجري على نحو مشابه جداً. إذ يعدنا قانون مور، مع محدودياته التي لا مناص منها في النهاية، بمعالجات متناهية في الصغر خلال سنوات قليلة. ونحن ننتج كل يومين من المحتوى الرقمي ما يعادل كل ما أنتجناه منذ فجر الحضارة حتى عام 2003، أي نحو 5 إكسابايت من المعلومات، مع وجود ملياري شخص فقط متصلين بالإنترنت من أصل سبعة مليارات. فكم من الأفكار الجديدة والمفاهيم والإبداعات الجديدة ستنتج عن الاندماج التقاني العالمي الحق؟ وبأي وتيرة ستزداد سرعة تأثيرها؟ إن وصول المزيد من الناس إلى العالم الافتراضي سيكون من حسن حظهم، ومن حسن حظنا أيضاً. فالمنفعة المشتركة لتشارك المعرفة البشرية والإبداع تتنامى بمعدل أسي.

ستكون تقانة المعلومات في المستقبل حاضرة في كل مكان؛ كالكهرباء اليوم. وسيكون وجودها بديهياً حيث تشكل جزءاً متكاملاً من حياتنا سنجد صعوبة في وصف الحياة من دونه لأطفالنا. ومع دفع الاتصالات لمليارات جديدة من البشر إلى الحظيرة التقانية، سندرك أن التقانة سرعان ما ستتدخل في جميع التحديات التي يفرضها العالم علينا. وستعمل الدول والشركات وكذلك المواطنون على جعلها جزءاً من كل حل.

ستنتهي جميع محاولات احتواء انتشار الاتصالات أو الحد من وصول الناس إليها بالفشل إذا أعطيت ما يكفي من الوقت. فالمعلومات - كالماء - ستجد دائماً منفذاً تتسرب منه. والدول والمواطنون والشركات والمنظمات غير الحكومية والمستشارون والإرهابيون والمهندسون والسياسيون والمخترقون، جميعهم سيحاولون التأقلم مع هذا التغير والتعامل مع آثاره اللاحقة، لكن أحداً منهم لن يستطيع التحكم به.

إننا نعتقد أن الغالبية العظمى من سكان العالم ستستفيد من انتشار الاتصالات، وستتمتع بمزيد من الفعالية وستتاح أمامها فرص أكثر، وستتحسن جودة حياتها. لكن على الرغم من هذه المنافع شبه الشاملة، لن تكون تجربة الاتصال واحدة.

فثمة نظام طبقي رقمي سيستمر لوقت طويل في المستقبل، وستتحدد تجربة الناس إلى حدٍّ كبير بالموقع الذي يجدون أنفسهم فيه ضمن هذه البنية. وستكون القلة القليلة في الأعلى معزولة إلى حدٍّ كبير عن تبعات التقانة الأقل إمتاعاً بفضل ثروتها والوصول المتاح لديها وموقعِها. وستقود الطبقة الوسطى في العالم الجزء الأعظم من التغيير، فمنها سيكون المخترعون، والقادة في جاليات الشتات، ومالكو المشاريع الصغيرة والمتوسطة. وهؤلاء هم الملياران من البشر المتصلين اليوم.

أما المليارات الخمسة التالية من البشر الذين سينضمون إلى القافلة، فسيعيشون تغيراً أكبر بكثير، وذلك ببساطة بسبب أماكن إقامتهم وأعدادهم. حيث سينعمون بأعظم المنافع التي تقدمها الاتصالات، لكنهم سيواجهون أيضاً أسوأ عيوب العصر الرقمي. فهؤلاء البشر هم الذين سيقودون الثورات ويتحدّون الدول البوليسية، كما أنهم سيكونون المواطنين الذين تتعقبهم حكوماتهم وتضايقهم حملات الكراهية على الإنترنت والذين سيتوهون نتيجة حروب التسويق. وستبقى تحديات كثيرة من عالمهم قائمة حتى مع انتشار التقانة.

فما الذي نعتقد أننا نعلمه حول عالم المستقبل؟ أولاً، من الواضح أن التقانة وحدها ليست الترياق الشافي لأمراض العالم، لكن الاستخدامات الذكية لها كفيلة بإحداث فرق في العالم. وفي المستقبل سيتقاسم البشر مع الحواسب المهام باضطراد وفقاً لما يجيده كل منهم. وسنستخدم الذكاء البشري من قدرة على الحكم والحدس وتمييز الفروق الدقيقة والتفاعلات البشرية الفريدة، كما سنستخدم الطاقة الحسابية المتمثلة في ذاكرة غير محدودة وقدرة معالجة غير محدودة وفي إنجاز مهام تمنعنا عنها البيولوجيا البشرية. وسنستخدم الحواسب لإيجاد تقاطعات توقعية بحجوم هائلة من البيانات لتتبع الإرهابيين والقبض عليهم، لكن سيبقى التحقيق معهم وطريقة معاملتهم بعد ذلك من اختصاص البشر وقوانينهم. ستمنع الروبوتات المقاتلة الوفيات بفضل دقتها العالية ووعيها للمحيط، لكن الحكم البشري سيقرر السياق الذي ستستخدم فيه والأفعال التي ستقوم بها.

ثانياً، لن يلحق العالم الافتراضي بنظام العالم القائم أو يصلحه، لكنه سيعقد جميع السلوكيات تقريباً. وسيفضل الناس والدول العوالم التي يكون لهم فيها قدر من السيطرة، أي ستفضل الشعوب العالم الافتراضي بينما ستفضل الدول العالم المادي، وسيبقى هذا التوتر قائماً طالما بقيت الإنترنت موجودة. وقد يكفي وجود جماهير تتوفر لديها الشجاعة الافتراضية لإطلاق ثورة، لكن الدولة ستستمر في اتباع الإجراءات الوحشية في القمع في الشارع. وقد تلجأ الأقليات إلى إقامة دولة افتراضية تقوي تآزرها، لكن إذا خرجت المغامرة عن مسارها، فقد ينتهي المشاركون وقضيتهم في وضع أسوأ مما كانوا عليه في البداية، في العالمين المادي والافتراضي، نتيجة لذلك.

ثالثاً، سيكون على الدول أن تمارس سياستين خارجيتين وسياستين محليتين، سياسة للعالم الافتراضي والأخرى للعالم المادي، وقد تبدو هذه السياسات متضاربة. وستشن الدول هجمات افتراضية على البلدان التي ما كان لها أن تحلم باستهدافها عسكرياً. وستسمح بالتنفيس عن المعارضة على الشبكة، لكنها ستخفر

شوارع المدينة بلا هوادة لقمع المعارضين الذين يتحدثون. وستدعم الدول تدخلات الاتصالات الطارئة من دون التفكير في وضع أقدام جنودها (أو روبوتاتها) على الأرض.

أخيراً، ومع انتشار إمكانيات التواصل والهواتف النقالة حول العالم، سينال المواطنون قدراً من السلطة لم ينالوه في أي حقبة سابقة في التاريخ، لكن سيكون لذلك ثمن، وخصوصاً في مجالي الأمن والخصوصية. فالتقانة التي نتحدث عنها تقوم بجمع الكثير من المعلومات الافتراضية وتخزينها (للمواقع التي كنت فيها في الماضي، أو تتواجد فيها في الحاضر، أو ستتواجد فيها في المستقبل إضافة إلى المعلومات التي تستهلكها) وستخزن جميعها لكي تعمل عليها هذه الأنظمة. ولم يسبق أن كان مثل هذا القدر من المعلومات متوفراً من قبل، وهو قد يستخدم ضدك في أي وقت. ستشرِّع الأمم معظم هذه المسائل وستختلف في سياساتها، ولن يكون الاختلاف بين الدول الديمقراطية وغير الديمقراطية فقط، بل أيضاً بين دول ذات أنظمة سياسية متشابهة. فخطر تسرب هذه المعلومات قائم، وعلى الرغم من توفر التقانة القادرة على حمايتها، ستزداد دائماً صعوبة الحفاظ على خصوصية المعلومات مع مرور الوقت نتيجة الخطأ البشري والنشاطات الخبيثة. وتتحمل الشركات المسؤولة عن تخزين هذه البيانات مسؤولية ضمان أمنها، ولن يتغير ذلك. وبينما تتحمل هذه الشركات مسؤولية الخصوصية الفردية أيضاً، فإنها تشارك المستخدمين هذه المسؤولية.

علينا أن نناضل من أجل الحفاظ على خصوصيتنا، وإلا فإننا سنفقدها، وخصوصاً في لحظات الأزمات الوطنية حيث سيصر صقور الأمن مع كل جريمة مروعة على أن الحكومات مخولة بالوصول إلى المزيد من المعلومات الخاصة، أو التي كانت كذلك. وسيكون على الحكومات أن تقرر أين توضع حدود الخصوصية الجديدة وأن تلتزم بها. وستحافظ تقنية التعرف على الوجوه على سبيل المثال على أمن البشر وتضمن أخذهم في الحسبان في كل شيء؛ بدءاً من الإحصاءات إلى التصويتات، عبر تسهيل التعرف على المجرمين والقبض عليهم، وبثني من ينوون ارتكاب أفعال إجرامية والترويج للسلامة العامة. لكنها قد تمنح الحكومات أيضاً القدرة على ممارسة المزيد من المراقبة على الشعب.

ماذا عن إمكانيات الحفاظ على الأسرار في المستقبل، والذي له الأهمية نفسها في عمل الأفراد والمؤسسات على حدٍّ سواء؟ ستؤدي القدرات الجديدة على تشفير الأسرار ونشر المعلومات بين الناس إلى بعض المشكلات غير الاعتيادية. فثمة مجموعات منعزلة (سواء أكانت من المجرمين أم من المعارضين) سيكون بمقدورها قريباً أن تعتمد سراً ما (ربما مجموعة من الرموز أو المستندات السرية)، وتشفره ثم توزعه عبر تسليم جزء من مفتاح التشفير لكل فرد في المجموعة. ويمكن بعدها للمجموعة أن تعتمد اتفاقية كشف مضمونة بالتبادل (أي أن يجمع الجميع مفاتيحهم الجزئية لكي يتم إطلاق البيانات). ويمكن استخدام مثل هذه الاتفاقية لتطويع الحكومة أو لإرهاب الأفراد. وإذا وضعت مجموعة مثل القاعدة يديها على بيانات حساسة مشفرة، مثل أسماء عملاء السي.آي.أيه المتخفين

ومواقعهم، فيمكنها توزيع نسخ منها على أتباعها مع مفتاح مشترك، والتهديد بإطلاق المعلومات إذا تعرض أي من أفرادها لهجوم.

إن ما سينشأ في المستقبل، وما حاولنا تلمسه هنا، قصة حضارتين: الأولى مادية تطورت على مدى آلاف السنين، والأخرى افتراضية لا تزال في طور التشكل في معظمها. وستتعايش هاتان الحضارتان تعايشاً سلمياً بطريقة أو بأخرى، حيث ستحد كل منهما من الجوانب السلبية للأخرى. وسيتمكن العالم الافتراضي من الهروب من قمع سلطة الدولة بأن يقدم للمواطنين فرص التنظيم والتمرد، بينما سيقوم مواطنون آخرون ببساطة بالاتصال والتعلم واللعب. وسيفرض العالم المادي قوانينه وقواعده التي تساعد على احتواء الفوضى في الفضاء الافتراضي بما يحمي الناس من المخترقين الإرهابيين ومن المعلومات المضللة، بل ومن السجلات الرقمية التي تشير إلى تهورهم في صباهم. وستصعب ديمومة الأدلة على مرتكبـي الجرائم التقليل من شأن أفعالهم أو إنكارها، مما سيفرض مستوى غير مسبوق من إمكانيات المحاسبة في العالم المادي.

ستؤثر الحضارتان الافتراضية والمادية إحداهما في الأخرى، وتساهم في تشكيلها. وسيحدد التوازن الذي تتوصلان إليه شكل عالمنا. وستكون النتيجة متعددة الأبعاد، من وجهة نظرنا، عادلة وأكثر شفافية وتشويقاً مما يمكننا أن نتخيل، وإن لم تكن مثالية. إذ سيتخلى المستخدمون طوعاً عن الأشياء التي يثمنونها في العالم المادي (من خصوصية وأمن وبيانات شخصية) بهدف الحصول على منافع التواصل مع العالم الافتراضي. لكنهم في المقابل إذا شعروا بأن هذه المنافع قد منعت عنهم، فسيستخدمون الأدوات المتاحة لهم للمطالبة بالمحاسبة بما يفرض التغيير في العالم المادي.

ليست المعدات الشبيهة بالخيال العلمي وأجهزة الإسقاط المجسمة هي ما يبعث على التفاؤل، بل القدرة على التحقق التي تعد بها التقانة والاتصالات ضد إساءة المعاملة والمعاناة والدمار في عالمنا. فعندما تحين الفرصة للكشف عن المعلومات، تصبح الإمكانيات غير محدودة. وأفضل ما يمكن لأي شخص فعله لتحسين جودة الحياة في العالم هو دفع عجلة الاتصالات والفرص التقانية. وعندنا تتاح إمكانية الوصول للناس، فإنهم يتكفلون بما تبقى. فهم يعلمون مسبقاً ما يحتاجون إليه وما يريدون بناءه، وسيجدون طرقاً للابتكار؛ حتى بأبسط الأدوات. ويمكن لأي شخص متحمس للرخاء الاقتصادي، وحقوق الإنسان، والعدالة الاجتماعية، والتعليم، وحق تقرير المصير أن يفكر في كيفية تمكن إمكانيات التواصل من مساعدتنا على تحقيق هذه الأهداف، بل وعلى تحقيق ما هو أبعد منها. ولا يمكننا أن نـزيل عدم المساواة أو استغلال السلطة، لكن الاحتواء التقاني كفيل بتحويل السلطة إلى أيدي الأفراد. لن يكون ذلك سهلاً، لكنه يستحق العناء.

انتهى

* وصلت الشهرة العالمية لنجم الكيه - بوب الكوري بسي إلى مستويات عالمية بين ليلة وضحاها تقريباً عبر الفيديو الذي أعده لأغنيته "غانغنام ستايل" حين أصبح فيديو اليوتيوب الأكثر مشاهدة على الإطلاق خلال فترة ثلاثة أشهر.
* الأجنحة الجراحية الروبوتية هي قيد التشغيل بالفعل في مشافي الولايات المتحدة وأوروبا اليوم.
* تقع معظم هذه التقنيات تحت مظلة أمثَلَة محركات البحث. فللتأثير على خوارزمية التصنيف التي تستخدمها لمحركات البحث، ثمة طريقة شائعة تتمثل في زراعة محتويات إيجابية حول الهدف (مثل اسم شخص)، والتشجيع على إقامة الروابط التي تشير إليه، وتحديثها باستمرار حيث يزيد احتمال أن تقيم عناكب محركات البحث المادة المعنية على أنها جديدة وذات شعبية، وهو ما يدفع المحتويات الأقدم والأقل صلةً بموضوع البحث إلى أسفل لائحة النتائج. كما يمكن التأثير على تصنيف المواقع بإضافة كلمات مفتاحية بارزة، وإضافة ارتباطات عائدة (أي ارتباطات قادمة إلى الموقع) في المواقع ذات الشعبية. وهي كلها تقنيات قانونية وتعتبر عادلة بشكل عام، إلا أنّ ثمة جانباً مظلماً لها (أمثَلَة القبعة السوداء) يتمثل في محاولات التلاعب بالتصنيف عبر ممارسات أقل قانونية تتمثل بتخريب محتويات أخرى (عبر الربط بينها وبين مواقع ذات إشارة حمراء مثل المشاهد الإباحية التي تشتمل على أطفال)، وإضافة نصوص مخفية أو التستر (أي خداع العنكبوت حيث يرى نسخة من الموقع بينما يرى المستخدمون نسخة أخرى).
* من الشائع أن ينسب هذا القول المأثور لستيوارت براند مؤسس فهرس هول إيرث كاتالوغ ومحرّره، حيث تم تسجيله في أول مؤتمر للقراصنة عام 1984.
* بينما يقصد بمصطلح "مخترق" في الأوساط التقنية الشخص الذي يطور شيئاً ما بسرعة وبنوع من العفوية، فإننا نستخدمه هنا بمعناه الدارج أي ولوج النظم من دون ترخيص.
* من بين التغريدات التي أرسلها مستشار تقانة المعلومات الباكستاني صهيب آثار ليلة مداهمة بن لادن: "حوامة تحوم فوق أبوتاباد في الواحدة من بعد منتصف الليل (هذا حدث نادر)".
* من اللافت أن هذا القانون برز خلال قضية في تكساس عام 2008، حين رفعت امرأة دعوى جماعية ضد موقع بلوك بوستر لمشاركته سجلات الاستئجار والشراء الخاصة بها على الفيسبوك من دون إذنها. وانتهت القضية بتراضي الأطراف.
* تتقاطع التقانة القابلة للارتداء مع صناعة ناشئة مشابهة هي التقانة التماسية، لكنهما ليستا مترادفتين. فالتقانة التماسية هي التقانة التي تتفاعل مع حاسة اللمس لدى المستخدم، ويكون ذلك عادة عبر النبضات أو الضغط. أما التقانة القابلة للارتداء فغالباً ما تتضمن أجزاء تماسية، لكنها لا تنحصر بهذه الأجزاء (مثل الستر التي يرتديها قادة الدراجات وتضيء في الليل)، كما أنه ليست جميع التقانات التماسية قابلة للارتداء.
* نسبة إلى جورج أورويل مؤلف رواية 1984. وهي رواية خيال سياسيّ، كان يتوقع من خلالها مصير العالم الذي ستحكمه قوى كبيرة تتقاسم مساحته وسكانه، ولا توفّر أحلامهم وطموحاتهم بل تحوّلهم إلى مجرّد أرقام في جمهوريات الأخ الأكبر الذي يُراقب كل شيء ويعرف كل شيء، حيث يمثل حكمه الحكم الشمولي.
* نوصي هنا بكتاب من يتحكم بالإنترنت: أوهام عالم بلا حدود الصادر عام 2006 لجاك غولد سميث وتيم وو، والذي يتابع هذا السيناريو بمزيد من الوضوح.
* إلا أنه ثمة أحداث أقل شأناً تشير إلى قدرة الحكومات على التلاعب بعملية التوجيه، بل وربما تشجيعها، بناءً على نطاقات الأسماء في بعض المناسبات. فقد حدث أكثر من مرة أن تم توجيه زوار موقع غوغل على الوب على نحو غامض إلى موقع بايدو، المنافس المحلي في الصين في مجال البحث.
* نحن نميز هنا بين الهجوم السايبري والإرهاب السايبري وفقاً للشخص أو الكيان الذي يقف خلف الهجوم وتقدير الدوافع. إلا أن كلا النوعين قد يظهران بطرق متشابهة جداً؛ مثل التجسس الاقتصادي.
* عندما سألنا رئيس الاستخبارات الإسرائيلية السابق، مائير داغان، عن هذا التعاون، كان تعليقه الوحيد هو: "هل تتوقع حقاً أن أخبرك؟".
* لا بد أن الحكومة الصينية ستضبط في النهاية متلبسة بهذه الهجومات الصناعية. وفي حال عرضت القضية على مجلس الأمن التابع للأمم المتحدة، فلا يمكن أن يتم اتخاذ قرار بشأنه بفضل سلطة الفيتو التي تتمتع بها الصين، لكن النتيجة ستبقى مع ذلك إحراجاً جيو - سياسياً جدياً.
* من الهام هنا التفريق بين وجود الأجهزة المخترقة داخل الشبكة الهدف أو خارجها. وهذا الأمر لا يهم كثيراً بالنسبة لأهداف هجمات حجب الخدمة العادية أو الموزعة، لكنه هام جداً في التجسس الصناعي؛ حين يكون الهدف هو الوصول إلى المعلومات. ففي هذه الحالات يجب على الأجهزة أن تكون داخل الشبكة.
* يعمل استخراج المعالم على اكتشاف وجود ميزات هامة أو غيابها، أو تحديد حالتها في مجموعة من البيانات. وفي مثالنا قد يعني ذلك اكتشاف مستوى بساطة الكتابة، أو تكرار كلمات مشحونة عاطفياً، وعدد الأشخاص المقتبس عنهم في النص؛ والذي يشير إلى مدى التأثر بهم.

_*_ عرضت المدونة التي تديرها شركة أبحاث الإنترنت رينسيس رسوماً بيانية مذهلة أظهرت الفصل شبه الفوري لمزودات خدمة الإنترنت المصرية عن الشبكة العالمية.

_*_* كان هناك استثناءٌ واحد لهذا الحجب الذي طال جميع مزودي خدمة الإنترنت، وهو مجموعة نور التي كانت تقدم الخدمة للعديد من المؤسسات المصرية البارزة مثل سوق الأسهم المصرية ومكتب الائتمان المصري، حيث سمح لها بالعمل بحرية لثلاثة أيام لاحقة.

_*_ يقوم المهاجمون السايبريون بتغطية آثارهم عبر توجيه البيانات إلى حواسب وسيطة بينهم وبين ضحاياهم. وتبدو هذه الحواسب الوسيطة (التي قد تكون عبارةً عن حواسب مخترقة في المنازل أو الشركات حول العالم) للضحايا وللخارجيين وكأنها مصدر الهجوم. وسيكون من الصعب بمكان اقتفاء آثار الهجمات السايبرية عبر الكثير من الطبقات الوسيطة للوصول إلى المصادر الحقيقية. وما يزيد الطين بلة هو أن المهاجم قد يشغل موجة تؤثر على المضيف المختَرَق ويُمطر الشبكة المختَرَقة ببياناتٍ مشوشة تضفي قناعاً على النشاطات التي ينوي القيام بها.

_*_ سيثبت مع ذلك أن التنفيذ سيكون صعباً، وذلك وفقاً لطبيعة الجريمة. فقد أدين كيفن ميتنك، الذي كان مخترق حواسب سيئ السمعة، وأمضى خمس سنواتٍ في السجن، ومنع بعدها - كجزءٍ من فترة اختباره - من استخدام الإنترنت أو الهاتف الخلوي، لكنه اعترض في النهاية على هذه القيود ضمن النظام القانوني وكسب دعواه.

_*_ أقل ما هنالك هو أن المنصات التي تنقل معلومات سرية مسروقة من الحكومات، كويكيليكس وتعاونيات المخترقين، تمكّن من التجسس أو تشجع عليه.

_*_ يعرف ذلك في الدوائر السياسية بأثر السي.أن.أن، وغالباً ما يرتبط بالتدخل الأمريكي في الصومال بين عامي 1992-1993. إذ يسود الاعتقاد بأن الصور التي كان يتم بثها على التلفاز والتي تُظهر صوماليين جائعين ويائسين هي التي حفزت جورج بوش الأب على إرسال قواته العسكرية إلى هناك. لكن، عندما قتل 18 من الحرس العسكري الأمريكي مع اثنين من الحلفاء الماليزيين في الثالث من تشرين الأول عام 1993، وانتشرت صور أحد الأمريكيين وهو يُسحل في شوارع مقديشو ووصلت إلى موجات الأثير، تم سحب القوات الأمريكية.

_*_ ثمة شركة ناشئة تدعى ستوريفول تقدم هذه الخدمة للكثير من محطات الأخبار الكبرى، ويعمل لديها صحافيون سابقون للتحقق من محتويات الوسائط الاجتماعية بدقة (يتم التحقق مثلاً من أن الطقس في فيلم فيديو على يوتيوب يتوافق مع حالة الطقس المسجلة في المدينة في اليوم الذي يفترض أن يكون الفيديو قد تم تصويره فيه).

_*_ سيذكر هواة الحاسب الدور المركزي الذي لعبته الوكالة في إنشاء الإنترنت أيام كانت تدعى وكالة مشاريع البحث المتقدمة (آربا).

_*_ تم نشر روبوتي باك.بوت خلال أزمة فوكوشيما النووية بعد الزلزال الذي ضرب اليابان عام 2011 لتدخل المحطة المتضررة، حيث كانت مستويات الإشعاع خطيرة على عمال الإنقاذ من البشر لو دخلوا وجمعوا بيانات بصرية أو بيانات تجمعها حساسات.

_*_ يؤكد العديد من مجندي القوات الخاصة الذين تحدثنا معهم مقولة سنغر.

_*_ استقينا هذه الواجبات من قائمة من عشر وظائف منوطة بالدولة من كتاب إصلاح الدول الفاشلة لكلير لوكهارت وأشرف غاني، مؤسّسي معهد فعالية الدولة.

_*_ من المعروف أن الصحفية ناعومي كلاين تطلق على هؤلاء الفاعلين اسم رأسماليي الكارثة في كتابها الاستفزازي مذهب الصدمة، حيث تحاجج كلاين بأن أنصار الاقتصادات النيوليبرالية يسعون لاستغلال بيئة ما بعد الأزمة لفرض نماذج السوق الحرة بما يعود عادةً بالضرر على النظام الاقتصادي القائم. وعلى غرار المعالجة النفسانية للصدمة يستخدم هؤلاء المتعصبون للسوق الحرة مظهر الصفحة البيضاء لإعادة تشكيل البيئة الاقتصادية على نحو عنيف.

_*_ تختلف تقديرات الوفيات البشرية في زلزال هاييتي في ما بينها اختلافاً كبيراً. إذ تعتقد الحكومة الهاييتية أن 316 ألف شخص قد قضوا نحبهم، بينما تضع مذكرةٌ مسربة من الحكومة الأمريكية الرقم بين 46,190 و84,961.